

TABLE OF CONTENTS

D3060/F1050 INSTRUMENTATION AND CONTROL (I&C)

1.0	APPLICATION OF THIS CHAPTER	3
2.0	ACRONYMS AND DEFINITIONS	5
3.0	CODES AND STANDARDS (PROGRAMMATIC AND FACILITY).....	8
4.0	DESIGN DOCUMENTATION	12
5.0	ENERGY CONSERVATION/SUSTAINABLE DESIGN	15
6.0	EQUIPMENT LOCATION.....	15
7.0	EQUIPMENT IDENTIFICATION	15
8.0	ENVIRONMENTAL CONSIDERATIONS.....	15
9.0	COMPUTER / CONTROL & DATA PROCESSING SYSTEMS AND EQUIPMENT	20
10.0	COLOR CONVENTIONS FOR PROCESS DISPLAYS	23
11.0	GROUNDING PRACTICES.....	25
12.0	ADDITIONAL REQUIREMENTS FOR SAFETY-RELATED SYSTEMS (PROGRAMMATIC AND FACILITY)	28

ATTACHMENTS

1. DESIGN GUIDANCE FOR INSTRUMENTED SYSTEMS USED IN SAFETY SIGNIFICANT AND HAZARDOUS PROCESSES
2. FAIL-SAFE DESIGN OF PROCESS CONTROL LOOPS
3. INSTRUMENTATION AND CONTROLS DESIGN REVIEWS
4. INSTALLATION AND CALIBRATION OF INSTRUMENTS
5. ALARM MANAGEMENT
6. INSTRUMENT LOOP DIAGRAMS
7. CONTROL LOGIC DIAGRAMS

RECORD OF REVISIONS

Rev	Date	Description	POC	OIC
0	5/22/02	Initial issue	Mel Burnett, <i>FWO-SEM</i>	Kurt Beckman, <i>FWO-SEM</i>
1	10/--/03	Added the following sections: Environmental Considerations, Computer/Control & Data Processing Systems and Equipment, Color Conventions for Process Displays, and Grounding Practices. Expanded the section (Additional Requirements for Safety-Related Systems) to include installation requirements and guidance for safety-related systems, the application of IEEE 384, and the application of ISA 84.01. Expanded/revised initial section contents for clarity and added information. Developed seven guidance based attachments to the I&C Chapter.	Mel Burnett, <i>FWO-DECS</i>	Gurinder Grewal, <i>FWO-DECS</i>

1.0 APPLICATION OF THIS CHAPTER

1.1 General

- A. The purpose of this chapter of the LANL Engineering Standards Manual (ESM) is to ensure I&C systems are designed to prevent accidents and mitigate consequences; are efficient, convenient, and adequate for good service; and are maintainable, standardized, and adequate for future expansion.
- B. All **facility**-related I&C design, material, equipment, and installations shall comply with site-specific requirements in this Chapter and [Chapter 1](#) of the ESM.¹ Requirements in this Chapter that also apply to **programmatic** work are addressed in Section 1.3.
- C. When new requirements are issued in the ESM, use the following to determine if the new revision is applicable to projects already started. For **small construction projects (programmatic or facility)**, the point used to determine applicability of new requirements is the FM's or Division Leader's approval to proceed with final design (beyond which, it is not necessary to apply the new requirements). Final design includes preparation of final working drawings, specifications, bidding documents, cost estimates, and coordination with all parties that might affect the project; development of firm construction and procurement schedules; and assistance in analyzing proposals or bids (from DOE O 4700.1). For **major projects** under the requirements of [LIR 220-01-01](#), Construction Project Management, refer to [LIR 220-03-01](#), LANL Engineering Standards Manual (Projects Underway), for application of the ESM.
- D. Where appropriate, guidance is provided to aid the cost-effective implementation of site-specific requirements and the requirements in the applicable codes. *Italicized* text identifies recommended guidance (not mandatory), based on good business practice and through lessons-learned at LANL. All other text in regular type indicates **mandatory** requirements unless prefaced with wording identifying it as guidance or a recommendation.
- E. In addition to new I&C installations, this chapter applies to some renovation, replacement, modification, maintenance, or rehabilitation projects.
 - 1. Bring existing I&C systems into compliance with current codes and requirements in this chapter when renovation work includes major replacements, modifications, or rehabilitation that exceeds 50% of the estimated replacement value² of the existing I&C system or subsystem³, and consider upgrading whenever work is initiated to address a safety issue or when safety-related systems will be effected by the modifications.
 - a. This requirement applies on a system or subsystem basis (e.g., a discrete HVAC control, process control, alarm, interlock, or indication system).
 - b. Systems and subsystems are listed in Section 210 of [Chapter 1](#) of the ESM.
- F. The adequacy of all design inputs is the responsibility of the designer/design agency. If the designer believes the ESM to be incorrect (e.g., compliance will cause a problem), it is their responsibility to bring the issue to the attention of the ESM Discipline POC (via the Project Manager if appropriate) for resolution.

- G. *Responsibility for the design of I&C, mechanical, and electrical systems can vary across organizations. Because this is a new chapter, the following table is included to show how LANL plans to distribute certain standards information between this and other ESM chapters. NOTE: Coordination between the discipline designers is essential to achieve the best systems.*

Electrical	I&C	Mechanical
<i>All power and control wiring</i>	<i>Controllers and processors for real-time control of mechanical, lighting, or building energy system monitoring</i>	<i>Fluid controlling devices such as valves and dampers with the associated actuators</i>
<i>Power supplies and UPS systems</i>	<i>Sensors and transmitters (temperature, humidity, flow, pressure, orifice plates, thermowells, flow measuring arrays and stations, etc.)</i>	<i>Local mechanical (non loop) indicators such as gauges and thermometers</i>
<i>Power switches, breakers, and relays</i>	<i>Self-contained controllers such as thermostats and humidistats</i>	<i>Instrumentation tubing and isolation valves</i>
<i>Electrical protective relays and devices</i>	<i>Reference pressure devices</i>	<i>Instrument air delivery systems</i>
<i>Motors, motor starters, and variable frequency drives (VFDs)</i>	<i>Low voltage switches and relays used as output devices to control mechanical systems</i>	
<i>Current and potential transformers used for electric metering and protection functions</i>	<i>Current transformers and relays used for status monitoring</i>	
<i>Electrical distribution monitoring and control</i>		

1.2 Exclusions

- A. The following are excluded from the requirements of this chapter.
1. Fire Protection systems and devices are covered by Chapters 2 and 7 of the ESM.
 2. Systems and devices providing security functions and controlled by S-Division.
 3. Systems and devices that have the primary purpose of controlling vehicular and/or pedestrian traffic.

1.3 Programmatic⁴

- A. The I&C chapter shall be applied to programmatic systems and components as follows:
1. Headings in this Chapter followed by “Programmatic and Facility” or a bold “P&F” indicate that subsection shall be complied with by all of LANL, including programs.

2. *Guidance: Programmatic personnel should review all topics in the chapter for relevant material when initiating any design task.*

2.0 ACRONYMS AND DEFINITIONS

<u>Acronym</u>	<u>Definition</u>
AHJ	Authority having jurisdiction.
ASHRAE	American Society of Heating, Refrigeration & AC Engineers
CFR	Code of Federal Regulation
Design Agency	The organization performing the detailed design and analysis of a project or modification.
Design Authority	The person or group responsible for the final acceptability of and changes to the design of a system or component and its technical baseline (typically the manager of engineering).
Design Documents	Design Documents are those design-related documents that define or otherwise control the final design, operation, or maintenance of a facility or program. Examples of design documents include drawings, as-builts, calculations, vendor manuals, equipment and document lists, studies, reports, and design specifications.
ESA	Engineering Sciences and Applications Division
ESM	Engineering Standards Manual
Facility	A synonym for Real Property and Installed Equipment. RP&IE is the land, improvements on the land such as buildings, roads, fences, bridges, and utility systems and the equipment installed as part of the basic building construction that is essential to normal functioning of a building space, such as plumbing, electrical and mechanical systems. This property/equipment is also referred to as institutional or plant and was formerly known as Class A. [DOE Order 4330.4B].
FWO	Facilities & Waste Operations Division
IEEE	Institute of Electrical and Electronics Engineers
ISA	The Instrumentation, Systems, and Automation Society
LCSM	LANL Construction Specification Manual.
LIG	Laboratory Implementation Guidance.
LIR	Laboratory Implementation Requirements.
Major Project	Construction project greater than \$500k (CPM LIR 220-01-01).

<u>Acronym</u>	<u>Definition</u>
Master Equipment List (MEL)	The MEL is a controlled hardcopy or electronic database of facility, LSG and applicable programmatic SSCs. The MEL captures and controls equipment information such as identification number, name, function, location, vendor data, design information, management level, and reference documentation.
ML-1	Management Level 1 (ML1) - Rigorous application of applicable codes, standards, procedural controls, verification activities, documentation requirements, and formalized maintenance program. Could include facility work for which independent review and management approvals for such things as design verification, procurement, fabrication, installation, assembly, and construction are considered essential. See LIG 230-01-02, Graded Approach for Facility Work.
ML-2	Management Level 2 (ML2) - Selective application of applicable codes, standards, procedural controls, verification activities, documentation requirements, and formalized maintenance program (i.e., certain elements may require extensive controls, while others may only require limited control measures). Could include facility work that may require independent review, management approval, and verification of design outputs, surveillance during procurement, fabrication, installation, assembly, and construction. See LIG 230-01-02, Graded Approach for Facility Work.
ML-3	Management Level 3 (ML3) - Application of appropriate codes, standards, procedural controls, verification activities, and documentation requirements that are consistent with recognized industry practices. Could include facility work that is normally manufactured, installed, assembled, and/or constructed in accordance with recognized codes and standards. See LIG 230-01-02, Graded Approach for Facility Work.
NFPA	National Fire Protection Association
OIC	Office of Institutional Coordination
OSHA	Occupational Safety and Health Administration
POC	Point of contact. For the ESM chapter/discipline Technical Committee POCs see http://www.lanl.gov/f6stds/pubf6stds/techcommittees.html
Programmatic	A synonym for Personal Property and Programmatic Equipment. PP&PE is equipment used purely for programmatic purposes, such as reactors, accelerator machinery, chemical processing lines, lasers, computers, machine tools, etc., and the support equipment dedicated to the programmatic purpose. This property/equipment is also referred to as organizational, research, production, operating or process and was formerly known as Class B. [DOE Order 4330.4B].

<u>Acronym</u>	<u>Definition</u>
Safety Class (SC)	Systems, structures, or components including primary environmental monitors and portions of process systems, whose failure could adversely affect the environment, or safety and health of the public as identified by safety analyses. [DOE 5480.30].
Safety-Related	A term meaning safety class, safety significant, and those ML-1 and ML-2 SSCs that could potentially impact public or worker safety or the environment in the same way as safety class or safety significant systems respectively.
Safety Significant (SS)	Structures, Systems, and Components that are not designated as Safety-Class SSCs but whose preventive or mitigative function is a major contributor to defense in depth and/or worker safety as determined from safety analyses. [10 CFR 830] As a general rule of thumb, Safety-Significant SSC designations based on worker safety are limited to those Systems, Structures, or Components whose failure is estimated to result in a prompt worker fatality or serious injuries or significant radiological or chemical exposures to workers. The term, serious injuries, as used in this definition, refers to medical treatment for immediately life-threatening or permanently disabling injuries (e.g., loss of eye, loss of limb).
Safety Significant Instrumented System (SSIS)	An SS system or 29 CFR 1910.119 hazardous process independent protection layer that requires instrumentation, logic devices and final control elements to monitor and detect a ML-2/SS event, and which will result in automatic or operator action that will bring the facility or process system to a safe state.
Small Construction Project	Construction project below \$500k.
Structure, System, and Component (SSC)	Structure, System, and Component are defined as “Structure is an element, or a collection of elements to provide support or enclosure such as a building, free standing tank, basins, dikes, or stacks; System is a collection of components assembled to perform a function such as piping, cable trays, conduits, or heating, ventilation, and air conditioning; and Component is an item of equipment such as a pump, valve, or relay, or an element of a larger array such as a length of pipe, elbow, or reducer.
System Design Description (SDD)	A document defining a facility safety or mission-important system. The system design description consolidates existing system designs and presents design basis requirements imposed on the system by governing criteria and analyses that dictate system design features and configurations.
WSS	Work Smart Standards. A set of Orders and national codes and standards in Appendix G of the LANL UC Contract.

3.0 CODES AND STANDARDS (PROGRAMMATIC AND FACILITY)

3.1 General

- A. Comply with the applicable portions of the latest edition of each code and standard listed below, referenced elsewhere in this chapter, and others as applicable, unless otherwise specified in the ESM or WSS. LANL Work Smart Standards are denoted as “WSS.”
- B. If there is a conflict between codes, standards, and LANL requirements such as this manual or project programming requirements such as Functional and Operational Requirements (F&OR), contact the LANL Engineering Standards Manual (ESM) Discipline POC⁵ for assistance in resolving the conflict. If a requirement in any LANL document exceeds a minimum code or standard requirement, it is not considered a conflict, but a difference, so comply with the most stringent requirements among the LANL documents.
- C. Requested variances and exceptions to the ESM requirements shall be prepared and submitted to the I&C POC for initial review and approval prior to his forwarding to the ESM Standards Manager, ESM OIC, and initiating and FWO Division Leaders per [LIR 301-00-02](#), Variances and Exceptions to Laboratory Operations Requirements, and [LIR 220-03-01](#), LANL Engineering Standards Manual.
- D. The graded application of codes and standards is not considered a variance to the LEM. When the graded approach is used to define the appropriate methodology for code and standard application, that methodology and rationale shall be formally documented and shall become part of the project design documents. The LANL Engineering Standards POC is the authority having jurisdiction for approval of the form and content of the documentation.
- E. **Codes of Record:** The codes and standards in effect when a facility design commences are considered the “codes of record” and often remain in effect for the life of the facility. Establishment and maintenance of the facility’s design basis, including “codes of record” shall be in accordance with [LIR 240-01-01](#), Facility Configuration Management. As determined by the Design Authority (System Engineer’s management) and the ESM I&C POC, the codes of record can be applied to later modifications, replacements, or rehabilitation less than 50% of the estimated replacement value when justifiable (when greater than 50%, the system shall be upgraded to current standards).
- F. When an existing I&C system is upgraded to Safety Significant/ML-2 or Safety Class/ML-1, the system owner shall perform a formal backfit analysis. The process shall determine if the I&C system complies with the current standards or establish the feasibility and cost effectiveness of redesigning the I&C system to comply with current standards. If the process finds the design complies with current standards, the analysis shall be submitted to the Design Authority for review and approval. If redesign is found to be necessary, feasible, and cost effective, the design agency shall commence design activities utilizing the current standards. If redesign is found not to be necessary, feasible or cost effective, the system owning division shall submit for a variance to the ESM requirements in accordance with [LIR 301-00-02](#), Variances and Exceptions to Laboratory Operations Requirements.

- G. **Listed Equipment:** All permanently installed programmatic I&C equipment and all ML-1, ML-2, and ML-3 facility I&C equipment shall be Nationally Recognized Testing Laboratory (NRTL) listed (e.g., UL, TUV, FM, etc.) or approved in accordance with [LIR 402-600-01](#) (Electrical Safety) and shall only be used for the purpose in which it is intended in accordance with its listing or Electrical Safety Officer approval.⁶ *Guidance: All other programmatic I&C installations should be Nationally Recognized Testing Laboratory (NRTL) listed equipment (e.g., UL, TUV, etc.) and should only be used for the purpose in which it is intended in accordance with its listing whenever possible.*
- H. **Prototype or Temporary Installations:** Prototype programmatic equipment or temporary (less than 90 days) facility or programmatic equipment must be installed in accordance with and meet the requirements of [LIR 402-600-01](#) (Electrical Safety). *Guidance: Peer review of the system design is especially useful and highly recommended for prototype installations.*
- I. **Online Codes and Standards:** Access to selected online national codes and standards are available to anyone with a LANL IP address or “smart card” at:
<http://lib-www.lanl.gov/infores/stand/standihs.htm>
- J. LANL Work Smart Standards (WSS) (Programmatic and Facility)⁷
http://labs.ucop.edu/internet/app_g/wss_lanl.pdf
- K. Comply with the latest edition and addenda in effect on the effective date noted in the WSS set, unless otherwise specified. Exception: Comply with the latest edition of the CFRs including all other applicable CFRs not listed in the WSS set.
1. *Guidance: CFRs with significant I&C design impact include OSHA (29 CFR 1910), especially subparts G, H, and Z regarding ventilation. CFRs available at <http://www.access.gpo.gov/nara/cfr/cfr-table-search.html#page1>*

3.2 LANL Engineering Standards

- A. Engineering Standards Manual (ESM), OST220-03-01-EM⁸
1. *Guidance: This chapter numbering generally follows the UNIFORMAT system promulgated by the Construction Specifications Institute (CSI) and further described in ASTM E1557.*
 2. Comply with standard detail drawings in the ESM unless referenced in *italicized* text. Edit the details to reflect the particular details of the project. *Guidance: The first digit of the standard drawing number, e.g., ST8XXX, designates the manual chapter (8 = chapter 8, I&C).*
- B. Construction Specifications Manual, OST220-03-01-CSM (Specification sections applicable to Programmatic work are clearly identified in that manual).
1. Comply with the LANL Construction Specifications Manual (LCSM) when writing and preparing a specification package, i.e., format, writing and editing, etc. *Guidance: The LCSM provides construction specifications that are referenced throughout the ESM. Specifications are preferred over extensive drawing notes.*

2. Number the specification sections in accordance with the CSI Master Format document, but do not renumber LANL Master Specs. *Guidance: LANL Master Specifications that do not conform to CSI numbers are being revised.*
3. Comply with specifications in the ESM unless referenced in *italicized* text. When editing these specifications to suit the project, add job-specific requirements and delete only those portions that in no way apply. To seek a variance from applicable requirements, contact the ESM discipline POC.

C. Drafting Manual, OST220-03-01-DM

4. Comply with the LANL Drafting Manual when creating or revising drawings for facility projects. *Guidance: This manual does not address weapons design work covered by ESA Division procedures. Use of the LANL Drafting Manual is recommended for programmatic work. The manual was completely revised in October 2001 and is periodically updated.*

- D. *Guidance: The LANL Standards are not intended to cover all design requirements and construction specifications necessary to provide a complete operating facility or system. The design organization is responsible for providing a complete design package.*

The above manuals are available at: <http://www.lanl.gov/f6stds/pubf6stds/xternhome.html>

3.3 DOE (Department of Energy) (Selected Orders)

The following directives are available at: <http://www.directives.doe.gov/serieslist.html>

- A. DOE O 420.1, Facility Safety, Attachment 2, Contractor Requirements Document (CRD) in its entirety with the following exceptions: **(Programmatic and Facility)**
1. Section 4.2, 2nd Paragraph (4)
 2. Section 4.2.1.9
 3. Section 4.2.2.4
 4. Section 4.3.2d(1)
 5. Section 4.3.2d(2), 3rd Sentence
- B. DOE G 420.1-1, Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria Guide for use with DOE O 420.1 Facility Safety **(Programmatic and Facility)**
- C. DOE M 440.1, Explosive Safety Manual (WSS) **(Programmatic and Facility)**
- D. DOE O 6430.1, General Design Criteria -- Division 13, Special Facilities, only (WSS).

3.4 National Codes and Standards – Task Matrix⁹

- A. The following application matrix identifies the minimum set of national codes and standards that shall be considered for I&C systems, consistent with their applicability for the specific technical or performance function. The requirements of the codes and standards shall be applied in a graded approach and documented in accordance with Section 3.1.D.

Table 3-1 Recommended Standards for I&C Systems			
Component / Function	ML-3 or General Service	ML-2 or Safety Significant	ML-1 or Safety Class
General	ISA 5.1 and 5.3; IEEE N323	ISA series especially 5.1, 5.2, 5.3, 5.4, and 84.01 ¹⁰ ; NFPA 70 and 110; ANSI C2, IEEE N323, 141, 142, 242, 493, and 1050; DOE G 420.1-1	ISA series especially 5.1, 5.2, 5.3, and 5.4; NFPA 70 and 110; ANSI N320; IEEE C2, N323, 141, 142, 242, 323, 336, 338, 344, 379, 384, 493, and 1050; DOE G 420.1-1
Scaling	ISA 67.04	ISA 67.04	ISA 67.04
Monitoring	HPS ASC N13; IEEE N42.18; NFPA 70; ANSI N13 series	HPS ASC N13; IEEE N42.17B, N42.18; NFPA 70; ANSI N2.3 ¹¹ , ANSI N13 series ANS 8.3 (criticality only)	HPS ASC N13; IEEE N42.17B, N42.18; NFPA 70; ANSI N2.3, ANSI N13 series ANS 8.3 (criticality only)
Programmable Digital Equipment	IEEE 1046 and 1289; ANS 10.5; NUREG 0700	IEEE 1046 and 1289; ANS 10.5; NUREG 0700	IEEE 1046 and 1289; ANS 10.5; NUREG 0700
Ventilation (Uniformat D3060)		ASME AG-1, N509 and N510	ASME AG-1, N509 and N510

Titles for Table 8-1

ANS 8.3, Criticality Accident Alarm System

ANS 10.5, Accommodating User Needs in Computer Program Development

ANSI C2, National Electrical Safety Code [NESC]

ANSI N2.3, Evacuation Alarm Systems

ANSI N13 series addresses radiation monitoring equipment

ANSI N320, Performance Specifications for Reactor Emergency Radiological Monitoring Instrumentation

ASME AG-1, Code on Nuclear Air and Gas Treatment

ASME N509, Nuclear Power Plant Air-Cleaning Units and Components

ASME N510, Testing of Nuclear Air-Cleaning Units and Components

DOE G 420.1-1, Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria Guide for use with DOE O 420.1 Facility Safety

HPS ASC N13, Guide to Sampling Airborne Radioactive Materials in Nuclear Facilities [Health Physics Society Accredited Standards Committee]

IEEE

N323, Radiation Protection Instrumentation Test and Calibration (ANSI/IEEE)

N42.17B, Radiation Instrumentation Performance Specifications for Health Physics Instrumentation – Occupational Airborne Radioactivity Monitoring Instrumentation

N42.18, Specification and Performance of On-Site Instrumentation for Continuously Monitoring Radioactivity in Effluents (ANSI/IEEE)

141, Recommended Practice for Electrical Power Distribution in Industrial Plants (IEEE Red Book)

142, Recommended Practice for Grounding of Industrial and Commercial Power Systems (IEEE Green Book)

242, Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems (IEEE Buff Book)

323, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

336, IEEE Standard Installation, Inspection, and Testing Requirements for Power, Instrumentation, and Control Equipment at Nuclear Facilities

338, IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

344, IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations

379, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems

384, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits

493, Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems (IEEE Gold Book)

1046, Application Guide for Distributed Digital Control and Monitoring for Power Plants

1050, IEEE Guide for Instrumentation Control Equipment Grounding in Generating Stations

1289, Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations

ISA [all formerly ANSI/ISA “S” series]

5.1, Instrumentation Symbols and Identification

5.2, Binary Logic Diagrams for Process Operations

5.3, Graphic Symbols for Distributed Control/Shared Display Instrumentation, Logic and Computer Systems

5.4, Instrument Loop Diagrams

67.04, Setpoints for Nuclear Safety-Related Instrumentation

84.01, Application of Safety Instrumented Systems for the Process Industries

NFPA 70, National Electrical Code [NEC]

NFPA 110, Standard for Emergency and Standby Power Systems; also NFPA 110A

NRC NUREG-0700, Guidelines for Control Room Design Reviews

4.0 DESIGN DOCUMENTATION

4.1 General

- A. The baseline Design Documentation (Design Input Specifications and Design Drawings) is to be established at a level commensurate with the management level/safety classification of I&C systems and/or devices in accordance with LIR240-01-01.2, Facility Configuration Management.
- B. Drawing content and format shall comply with the LANL Drafting Manual including its Mechanical section (*Section 305*) and Electrical section (*Section 306*).
- C. A Design Input Specification shall be developed for Safety-Related systems to include, as applicable, the following items:¹²
 1. Performance requirements for all plant operating conditions (accident and normal) wherein the equipment is expected to perform an intended function.

2. Ambient and process operating conditions including the measured variable for each of the applicable operating modes and conditions.
3. The minimum and maximum ambient temperatures to which the I&C system devices will be subjected.
4. The minimum and maximum pressures to which the I&C system devices will be subjected.
5. The minimum and maximum relative humidity to which the I&C system devices will be subjected.
6. The cumulative dosage levels (alpha, beta, and gamma) and maximum dose rates to which the equipment will be subjected under the operating conditions.
7. Concentration and duration of chemical exposure to which the equipment will be subjected.
8. All electrical power transients and normal power fluctuations to which the I&C system devices may be subjected.
9. Structural/Vibratory loads to which the instrumentation and control system components, enclosures, or supports will be subjected.

Guidance: The above items that constitute a Design Input Specification should be addressed for any I&C system, as applicable or practical.

- D. A System Design Description shall be developed for Safety-Related I&C systems, or those I&C systems that provide a mission critical, defense in depth, or worker safety function or whose failure may impact the operation of safety related SSCs.¹³ The system design description shall be based on DOE-STD-3024 and shall establish the purpose (design function) and safety classifications for the I&C components, and at a minimum, shall contain the following content:¹⁵

1. System and Component Functions
2. System and Component Design Requirements or Constraints
3. Operation Description
4. Set Points and System Limitations (Expected Values or Ranges)
5. Expected System Upsets and Methods/Procedures for Recovery
6. Maintenance Requirements and Recommendations
7. Bases for Design Requirements
8. Interface Requirements
9. References

- E. Any necessary calculations shall be performed and documented according to FWO-DO-603, "Calculations", or AP-ENG-007, "Developing and Revising Engineering Calculations".

F. *Guidance: As part of the Project Record File, when required, the following documentation should be obtained from the Manufacturer of I&C system devices, as applicable:*¹⁶

1. *Mounting connection details*
2. *Weight and center of gravity*
3. *Service connections, size, type, and locations*
4. *Materials of construction*
5. *Design life*
6. *Environmental and seismic qualifications*
7. *Mounting restrictions and instructions*
8. *Loop and logic diagrams*
9. *Electrical schematic and wiring drawings*
10. *Panel general arrangement and construction drawings*
11. *Instrument piping and tubing drawings*
12. *Certificate of conformance*
13. *Calibration procedures and data*
14. *Panel mounted instrument list including nameplate engraving*
15. *Maintenance and surveillance requirements*
16. *Recommended spare parts listing*
17. *Specification data sheets for components, parts, or system*

G. *Guidance: ISA-20-1981, "Specification Forms for Process Measurement and Control Instruments, Elements, and Control Valves" should be used to assist in procurement of instrumentation equipment. These data sheets are available from FWO-DECS.*

4.2 Sealing Construction Documents (Programmatic and Facility)

A. Comply with the New Mexico Engineering and Surveying Practice Act (Chapter 61, Article 23 NMSA 1978), <http://www.state.nm.us/pepsboard/Act.htm>. All plans, designs, drawings, specifications, or reports prepared for LANL by consultants or contractors that are involved in the practice of engineering shall bear the seal and signature of a professional engineer in responsible charge and directly responsible for the engineering work.

1. University employed engineers, performing engineering services involving the operation of LANL, on LANL property, are exempt from the licensing requirements of the New Mexico Engineering and Surveying Practice Act.¹⁷

5.0 ENERGY CONSERVATION/SUSTAINABLE DESIGN

- A. Comply with ASHRAE Standard 90.1. This standard provides minimum energy-efficient requirements for the design and construction of new buildings and their systems, new portions of buildings and their systems, and new systems and equipment in existing buildings.¹⁸
- B. Provide a computerized Facility Management System in all new, air conditioned buildings larger than 10,000 square feet.¹⁹
- C. HVAC control systems design, materials, and construction are an integral component of sustainable design. Design I&C systems and specify equipment for compatibility with the building and site aesthetics, lighting and electrical systems requirements, and indoor environmental quality requirements to ensure that multi-discipline whole-building sustainable design practices are followed.
 - 1. *Guidance: Refer to the Green Building Council's LEED rating system and other resources at <http://www.usgbc.org/resource/index.htm> and DOE/GO-102001-1165, Greening Federal Facilities; An Energy, Environmental, and Economic Resource Guide for Federal Facility Managers and Designers. <http://www.nrel.gov/docs/fy01osti/29267.pdf>*

6.0 EQUIPMENT LOCATION (PROGRAMMATIC AND FACILITY)

- A. I&C equipment shall be accessible for inspection, service, repair, and replacement without removing permanent construction, as required by code and as recommended by the manufacturer.²⁰
 - 1. If Safety-Related I&C equipment is not accessible with a man-lift or rolling platform, provide permanent OSHA compliant structures for access to equipment installed 12 feet or higher above finished floors (e.g., controllers, transmitters, valve/damper actuators, etc).²¹ *Guidance: This requirement should be considered, not only for Safety-Related equipment, but for any I&C component that is located 12 feet or higher, especially if frequent inspections are necessary.*

7.0 EQUIPMENT IDENTIFICATION (PROGRAMMATIC AND FACILITY)

- A. Identify major I&C equipment in accordance with the nomenclature indicated in LANL Engineering Standards Manual, [Chapter 1](#), Section 230, Component Nomenclature.
- B. Label I&C equipment in accordance with ESM Chapter 1, Section 240, Labeling (future), LANL [Construction Specification](#) 15075, Mechanical Identification, and LANL Construction Specification 16195, Electrical Identification as applicable.²²

8.0 ENVIRONMENTAL CONSIDERATIONS²³ (PROGRAMMATIC AND FACILITY)

The requirements identified within this section are for Safety-Related I&C systems or those I&C systems that provide a mission critical, defense in depth, or worker safety function or whose

failure may impact the operation of Safety-Related SSCs. For other non-safety I&C systems, all items in this section shall be interpreted as guidance that establishes sound engineering practice for the proper and reliable performance of I&C systems.

8.1 General

- A. The environmental conditions in which I&C equipment must operate or which can affect the proper or continued operation of I&C equipment shall be clearly identified and considered in I&C design and equipment selection. Normal ambient, abnormal operating, climatic and event conditions shall be evaluated in the identification of applicable environmental conditions.

Guidance: The environmental factors that should be considered when selecting equipment location or equipment for a location include, but are not limited to, the following:

1. *Temperature and/or Humidity Extremes*
 2. *Barometric Pressure Variations*
 3. *Airflow*
 4. *Corrosive Atmospheres*
 5. *Area Flooding*
 6. *Acoustic Noise*
 7. *Electronic Noise, or Electromagnetic Interference (EMI)*
 8. *Power Supply Quality (electrical surges, frequency variations, etc.)*
 9. *Grounding*
 10. *Lighting*
 11. *Lightning Protection*
 12. *Physical Security*
 13. *Vibration*
 14. *Interference from Large Motors and Power Feeders*
 15. *Chemical and Particulate (dust) Contamination*
- B. The I&C equipment that is required to meet performance specifications may necessitate a specific type of environment, or in other cases, the environment may limit the choice of equipment. Where I&C equipment cannot be found that will provide the required performance in the environmental conditions present, alternate means shall be provided such as heated, cooled, waterproof, corrosion protective and similar enclosures. For enclosures or other environment protective devices, their effect on equipment performance, ability to test, and effect on calibrations shall be evaluated.
- C. All environmental restrictions imposed by the manufacturer of the equipment shall be met. If several types of equipment are to be located within the same environment, the environment must satisfy the most restrictive of all the equipment specifications.

Guidance: In extreme cases, the equipment climate may require very close control over all environmental aspects. In some instances, sensitive equipment may be placed in a sealed enclosure, so that only a relatively small volume would need to be protected. The more rugged equipment, such as programmable controllers, industrialized PCs, or MIL-Spec equipment, can usually be installed and maintained under the existing ambient conditions. Hazardous areas may necessitate the use of intrinsically safe equipment, explosion-proof enclosures, sealing and purging, etc.

- D. If I&C equipment is to be located in Class I, Divisions 1 and 2; Class II, Divisions 1 and 2; or Class III, Divisions 1 and 2 locations, where fire or explosion hazards may exist due to flammable gases or vapors, flammable liquids, combustible dust, or ignitable fibers, the requirements of NFPA 70 (NEC) – Articles 500 through 504 shall be met.

Guidance: ANSI/ISA-RP12.06.01, "Wiring Practices for Hazardous (Classified) Location Instrumentation – Part 1: Intrinsic Safety", provides guidance in the design, installation, and maintenance of intrinsically safe I&C systems for hazardous (classified) locations. This recommended practice should be used in conjunction with the requirements of Article 504 of the NEC.

8.2 Specific Considerations

- A. Temperature: The temperatures to which I&C equipment may be exposed in the application shall be clearly identified. The temperatures of concern shall be evaluated against the specified operational temperature requirements for the selected equipment to ensure compatibility. If equipment selection is not conducive to the given temperature conditions, alternate measures shall be taken, such as the use of the temperature-controlled enclosures.

Guidance: The temperature of concern is the temperature of the medium (whether air or liquid) which affects or cools the equipment. In regard to fan-cooled equipment, the temperature of concern is that of the air entering the equipment. Operational temperature requirements for equipment is normally well defined in the manufacturer's literature. Two separate temperature ranges are typically specified, one for when the equipment is in operation and another for when the equipment is powered-down, shipped, or in storage. Operating temperatures may also be specified as ambient, which refers to the surrounding temperature, and process, which refers to the process media being measured. The manufacturer's equipment specifications may also include a maximum allowable rate of change of temperature, given in degrees per hour.

- B. Airflow: The design and control of airflow systems shall consider both equipment locations and normal airflow patterns.

Guidance: Airflow in fan-cooled and convection-cooled equipment is generally vertical through the enclosure and can be from either the bottom or top. For rooms containing equipment with downward airflow, the air supply should be overhead and the return plenum should be low or in the floor. If a raised floor is in place, the space under the floor may provide the return plenum. For upward airflow, the use of the sub floor space as a supply plenum is to be avoided because it requires additional design considerations and continuing maintenance to prevent the infiltration and accumulation of dust, dirt, and moisture under the floor.

- C. Relative Humidity: The selection of equipment shall consider the relative humidity to which I&C equipment may be exposed in the application. If necessary, the design shall incorporate the use of humidity control equipment to assure operation within the defined limits for the selected equipment.

Guidance: The operating relative humidity requirement for equipment is normally well defined in the manufacturer's literature and typically given as an operating range and a maximum time rate of change. Limitations may be given for shipping and storage as well as for operation. Typically, the desired operating range is about 40 – 60 percent. Low relative humidity (less than 30 – 40 percent) can result in system errors or shutdowns due to generation of static electricity. High relative humidity can lead to condensation.

- D. Particulate Contamination: The presence of particulate matter (dust or dirt) shall be considered for its affect on I&C equipment.

Guidance: Dust, grit, and sand present at the inlet of process media sensing devices can prevent the equipment from performing its function. Dust build up decreases the ability of electrical components to shed their heat, which decreases longevity. In fan-cooled equipment, the accumulation of dust on filter media will reduce airflow and cause overheating. If the dust is conductive, it can cause faults; if nonconductive, it can infiltrate and insulate switches and contacts. Careful, meticulous sealing of all equipment enclosure openings will reduce contaminant infiltration.

- E. Chemical Contamination: Consideration shall be given to potential chemical contamination and corrective action shall be taken to limit any potential contamination below levels that could adversely affect equipment performance.

Guidance: Certain chemicals, including sulfur dioxide, oxides of nitrogen, hydrogen sulfide, and ammonia, are known to affect electronic equipment at concentrations safe for human occupancy. Most corrosion processes accelerate rapidly at increased temperatures or humidity level (or both). Some maximum allowable levels recommended by equipment manufacturers are below levels that can be readily measured.

- F. Vibration and Shock: The proposed location of I&C equipment shall be evaluated for potential sources of vibration and shock, such as nearby heavy rotating or stamping equipment or heavy mobile traffic. Consideration shall be given to potential vibration and shock sources when mounting I&C equipment to assure operation within the equipment manufacturer's defined limits.

Guidance: Continuous vibration can cause slow degradation of contacts and any mechanical parts. Shock can instantaneously change an instrument adjustment, as well as cause effects similar to vibration. It is usually more practical to relocate equipment or to apply controls at the vibrating equipment than to try to isolate the equipment from the vibration.

- G. Power Line Conditioning and Backup: The equipment manufacturer's power requirements shall be met. In many cases, meeting these requirements involves more than just supplying the appropriate voltage and ampacity ratings. Frequently a special type of receptacle is required, which is usually well defined in the manufacturer's literature. Transient Suppressors may be required depending on the type of device. Tolerance to voltage transients and brownouts are also typically defined in the manufacturer's literature. ANSI standards permit user line voltage to be as much as 11.7 percent below nominal. Brownouts may cause additional voltage reductions of 3 to 10 percent. These reductions may severely disrupt equipment operations and may necessitate the need for power conditioning and/or backup power supplies.

Guidance: Certain critical systems should be able to operate through a power dip or an extended power outage; these should be provided with a backup power supply. For less critical systems, a packaged power conditioning system should be considered.

- H. Electromagnetic Interference (EMI): The proposed location of I&C equipment shall be evaluated for potential sources of EMI and consideration shall be given to its effect on the operation of the equipment. EMI results from electromagnetic emissions generated by and coupled to equipment or systems (or both).

Guidance: Common EMI sources include thunderstorms, high voltage power lines, power tools and manufacturing machines, relays, contactors, motors, vehicle ignitions, and arc welders. Isolation, shielding, and grounding may be required to prevent expected problems.

- I. Radio Frequency Interference (RFI): The proposed location of I&C equipment shall be evaluated for potential sources of RFI and consideration shall be given to its effect on the operation of the equipment. RFI results from electromagnetic fields generated by communication and electronic equipment.

Guidance: Common RFI sources include hand held radio transmitters, cell phones, proximity to radio or television disks or towers, and proximity to communication relay disks or towers. Generally, RF fields within the facility should not exceed 0.5 v/m. Not more than 1V RMS, in the frequency range of 10kHz to 3 MHz, should exist on the ac connection points to the system. Isolation, shielding, and grounding may be required to prevent expected problems.

- J. Static Electricity: The potential for static electricity problems shall be determined and if present, prevented or corrected.

Guidance: Static electricity can have a significant affect on digital equipment and equipment connected to explosive applications or in explosive environments. The catastrophic effect is the breakdown and permanent damage of semiconductor devices. The transient effect is the introduction of extraneous logic signals or voltages induced on ground or signal wiring, which can result in operational error.

9.0 COMPUTER / CONTROL & DATA PROCESSING SYSTEMS AND EQUIPMENT (PROGRAMMATIC AND FACILITY)

9.1 General

- A. The requirements and guidance identified within Section 8.0, Environmental Considerations, are applicable to computer/control and data processing systems and equipment. The following is provided as a supplement to Section 8.0 to specifically highlight the needs of digital and computer based systems. When selecting a location for this type equipment, the environmental factors identified within this section shall be addressed.

Guidance: The following represents input and/or guidance in addition to that identified within Section 8.0, Environmental Considerations, for control/computer room design, equipment location, and equipment installation:

1. *Temperature: Although cooler temperatures are preferable for computers, operation near the center of the defined range is recommended to strike a balance between individual comfort, energy efficiency and computer operation.*
2. *Temperature: For rotating media storage (e.g., disk drives), the manufacturer typically gives a maximum allowable rate of temperature change. In such equipment, the disk and drive mechanism should be kept at the same operating temperature and rapid temperature transients should be avoided. This is true for most all I&C signal processing equipment.*
3. *Relative Humidity: Magnetic storage media should not be contained within areas that could experience rapid changes in relative humidity. The manufacturer of such equipment typically identifies the maximum allowable time rate of change.*
4. *Particulate and Chemical Contamination: Computer/control and data processing equipment, especially moving magnetic storage devices (disk drives and tapes), is typically sensitive to damage caused by contaminant infiltration. Filter replacement and dust or particulate removal should be performed regularly in all computer equipment cabinets as part of a preventative maintenance program. General cleanliness and good housekeeping practices should be enforced. Equipment and partitions should be arranged to minimize the number of times doors are opened. The use of the room as a thoroughfare should be prohibited. In some installations, a remote console will solve contaminant infiltration problems.*
5. *Vibration: Careful attention should be given to potential sources of vibration when selecting a location for disk drives, which are particularly sensitive to vibration effects.*
6. *Electrical Power: Design provisions or operating procedures (or both) should be established to prevent vacuum cleaner or similar motor driven equipment from being powered from the computer power conditioning system. A disconnecting means should be provided to disconnect the power to all electronic equipment in a data processing room. This disconnecting device should be controlled from locations readily accessible to the operator at the principal exit doors. There should also be a similar device to disconnect the HVAC system servicing the area. Article 645 of the Nation Electrical Code provides specific requirements for the electrical wiring associated with computer systems.*

7. *Interference: A computer and peripherals can erroneously interpret radiated energy from EMI or RFI sources as data or control signals. The result can appear as I/O problems, analog to digital conversion inaccuracies, or outright processor failures. The random nature of the interference makes failure diagnosis difficult. Computer/control and data processing equipment should be located away from sources of EMI or RFI. When this is not practical, it may be necessary to enclose vulnerable computer components within an RFI-shielded enclosure or area.*

9.2 Computer/Control Rooms

A. The following items shall be addressed in the design of computer/control rooms:²⁴

1. Proper space allocation for computer equipment, consoles, storage area (for manual, documents, listings, maintenance equipment, etc.), environmental conditioning equipment (air and electrical power conditioning), fire protection equipment, and power distribution.
2. Room accessibility for both operating and maintenance personnel. *Guidance: The addition of interior windows, where appropriate, can reduce unnecessary traffic (e.g., room security, safety of personnel, etc. can be observed without entering the room).*
3. Space allocation for any potential expansion.
4. Suitable access and easy loading areas for equipment.
5. Adequate and convenient wire paths for installing signal, data, process control, safety, and associated power wiring to and from the computing systems. *Guidance: A "raised floor", with removable panels, provides the most convenient method for the installation of computer room wiring. Unrelated services, such as power conductors, water and steam piping, etc., should not be installed in the computer room or its included spaces and specifically should not be present overhead data processing equipment or computer/control rooms. If unrelated services must be installed, the design should incorporate appropriate measures to protect the computer equipment.*
6. Data handling and analysis area. This is normally a small area for a conference table and chairs where computer printouts and reports may be laid out for analysis.
7. Emergency lights, fire doors, power and air handling interlocks, etc.
8. Radio Frequency Interference (RFI) and Electromagnetic Interference (EMI) shielding, if required.
9. Fire codes and requirements.
10. Telephone and intercommunication systems.
11. Adequate and proper lighting. *Guidance: Two levels of lighting may be necessary; one for normal operation and one for maintenance. The Illuminating Engineering Society (IES) Lighting Handbook includes both quantitative and qualitative design data for various lighting needs. Where CRTs are in use, glare and reflection should be eliminated. Dimmer switches are sometimes used to reduce glare. Note, however, that SCR dimmer controls can be a source of RFI and should be avoided.*

- B. The computer/control room design, location, and access points shall be evaluated for the potential presence or introduction of contaminants through materials of construction, ventilation systems, transfer from adjacent areas or from workers and visitors. Any potential source of contamination that would affect the proper operation or reliability of the equipment shall be prevented by design, protective measures, or administrative procedures.²⁵

Guidance: The following should be taken into consideration to prevent the presence or introduction of contaminants within a computer/control room:

1. *Only materials that do not produce contaminants should be used in control/computer room construction. Sprayed-on acoustical ceiling and mineral-based drooped ceiling tiles should be avoided because they tend to flake. Glass fiber tiles that produce abrasive particles and floor covering that tend to crack or crumble should be avoided. Also, carpets should be of a quality that minimizes the release fibers and particulate. All exposed concrete should be sealed.*
 2. *Specially treated (impregnated) mats should be placed at each entrance to reduce the amount of dust tracked in by personnel.*
 3. *The use of a computer/control room as a gathering place should be avoided. However, the room may need to be used as a rally point for personnel in the event of a fire, explosion, or fume release. In such cases, provisions necessary for employee protection as well as for equipment protection should be considered.*
 4. *All floor or other cable trays should be capable of being kept clean and free of dirt, grit, or debris.*
 5. *Maintaining the computer/control room at a positive pressure may be considered as a means of preventing the entry of contaminants. In this application, special attention must be given to the quality of the inlet air and its source.*
- C. The potential for static electricity in computer/control rooms shall be eliminated to the maximum extent possible in room design and equipment location. Where a potential may exist for the generation of static electricity that could be detrimental to equipment operation, measures shall be taken to minimize the potential for static electricity generation. This may take the form of material and equipment prohibitions, temperature and humidity control, grounding methods, etc.²⁶

Guidance: The following should be taken into consideration to prevent static electricity in computer/control rooms:

1. *For control of static electricity, carpet is not the preferred floor covering for computer/control rooms. If carpet is used, steps should be taken to reduce static buildup. Certain carpets are given anti-static properties by the incorporation of metallic fibers during manufacture or treatment with anti-static agents. Anti-static sprays are available for use on existing carpet. Wax buildup on tile floors also increases surface resistivity and leads to static problems. The remedy is to forego waxing or to use a wax formulated for high conductivity.*
2. *Furniture in the vicinity of digital equipment should be chosen carefully. Seat covers of plastic are normally more likely to generate static charges than cloth covers. Wheels and casters should contain conductive material and should be lubricated with graphite or conductive grease. Rubber or plastic feet should be avoided.*

3. *Storage space may be required for operating supplies and storage media, spare parts and components, and backup software. These items may need protection from static electricity buildup both in storage and when handled. The manufacturer's recommendations for both the use and storage of these items should be followed.*
 4. *Personnel grounding straps and insulating footpads may be necessary for especially sensitive processes or operations. Equipment sensitivity of this nature should be identified in design and operation documentation.*
- D. *Guidance: Locating a computer/control room in an area subject to flooding should be avoided. Where this is not realistic for all possible conditions and flooding is possible, alternative measures should be taken, such as constructing a raised floor for the computer/control room. For raised-floor computer/control rooms, the installation of an alarm system initiated by water detectors located under the raised floor should be considered.*

10.0 COLOR CONVENTIONS FOR PROCESS DISPLAYS²⁷ (PROGRAMMATIC AND FACILITY)

- A. Within a given facility, color conventions for process displays shall be consistent, simple, and unambiguous.
- B. Color coding shall be redundant with some other display feature (e.g., text, symbol, shape, size, intensity, or inverse video) such that all necessary information is available on a monochromatic display or printout, or when viewed by a user with color vision impairment.
- C. The color conventions given in the following, Table 10-1, shall be used for process displays.²⁸ *Guidance: Color identified in the last column as "Contrasts Well With" are recommendations, not requirements. However, color combinations should be carefully selected to ensure good contrast (i.e., do not use red characters on a green background).*

Table 10-1				
Color Conventions for Process Displays				
Color	Generic Meaning	Associated Meanings	Attention Getting Value	Contrasts Well With
Red	Unsafe	Emergency Danger High Priority Alarm Closed / Off / Stopped (inactive) Closed / On / Flowing (electrical power distribution)	Good	White
Yellow	Caution	Hazard Second Priority Alarm Abnormal State	Good	Black Dark Blue
Green	Safe	Safe Satisfactory Open / On / Flowing (active) Open / Off / Stopped (electrical power distribution)	Poor	White
Light Blue (cyan)	Static and Significant	Equipment in Service Major Labels	Poor	Black
Dark Blue	Non Essential	Equipment in Standby Labels, Tags	Poor	White
Magenta	Radiation	Radiation Alarm / Caution Questionable Values	Good	White
White	Dynamic Data	Measurement and State Information System Messages Trend Active Sequence Step	Poor	Black Green Dark Blue Magenta Red
Black	Background		Poor	White Yellow Light Blue

- D. For ML-2/Safety Significant or ML-1/Safety Class structures, systems and components, a review shall be conducted during the design process for proper application of color and shape conventions from a human factors perspective.
- E. *Guidance: The number of colors used for coding should be kept to the minimum needed for providing sufficient information (usually no more than eight colors). Decorative use of color should be eliminated.*
- F. *Guidance: Highly saturated colors should be used for coding to provide good contrast from each other and their backgrounds.*

- G. *Guidance: Gradual changes in color intensity should not be used to indicate relative values of variables.*
- H. *Guidance: Flashing or audible indications should be included when display items require immediate operator attention, such as alarms.*

11.0 GROUNDING PRACTICES

- A. A. Grounding systems for I&C and Computer/Data Processing systems and equipment shall be provided to minimize damage to equipment, interference with equipment operation or signal processing, and shock or other electrical hazards to personnel. Federal Information Processing (FIPS) Pub 94 provides a guide, checklist and evaluation criteria for specifying power and related grounding and life-safety requirements for the design, installation, and operation of Automatic Data Processing (ADP) systems. This standard shall be used in conjunction with the mandatory power-grounding requirements of NFPA 70 - Article 250, IEEE 142, IEEE 1100, and IEEE 1050.

Guidance: Grounding systems should be designed to meet the following major goals:

1. *Provide for personnel and equipment protection and life-safety required by various regulatory agencies.*
 2. *Maintain all equipment and circuits at the same reference ground potential.*
 3. *Provide a safe, high ampacity fault return path for those power distribution systems that have the source or generating system referenced to ground.*
 4. *Maintain a low inductive loop area between the power distribution system and the fault return path for equipment that has a potential for high fault currents.*
 5. *Provide a low impedance leakage path for any static charge that may accumulate on equipment.*
 6. *Provide a low impedance discharge path for energy storage devices such as capacitors and inductors that are installed for the suppression of high voltage transients or electrical noise.*
 7. *Minimize noise interference in instrumentation systems by providing common reference planes of low relative impedance between devices, circuits, and systems.*
 8. *Assure that all ground system conductors that must carry high frequency signals (greater than 10 kHz) are selected for low inductance characteristics. At 1 Megahertz, the impedance of an average length ground conductor is around 4,000 ohms.*
- B. Conductive enclosures that contain I&C and computer/data processing system components shall be appropriately connected to ground to ensure that shock hazard risks are minimized for personnel.²⁹

Guidance: The connection should provide a low resistance path to ground for any fault currents that may be produced by mechanical failures, insulation failures, component failures, accidents, etc. Low resistance paths to ground maintain low potential differences between metal components and reduce the chances of a fault-induced current flowing through personnel in contact with system components. Grounding is especially important in an environment where conductive elements may be present in the flooring, piping, ductwork, or other equipment.

- C. The grounding of I&C and computer/data processing systems shall provide protection against self or adjacent equipment generated or induced electrical noise.

Guidance: The following information provides insight on potential sources of electrical noise, its effects on I&C and/or computer/data processing systems, and the application of proper corrective grounding techniques:

1. Computer/control and data processing systems utilize high speed, low level switched signals for operation. At the high frequencies at which these systems operate, electrical noise will propagate, traveling between two conductors or between an insulated ground conductor and other grounds or metallic components in the area. It is important that the system ground be connected in such a way that it does not act as part of a transmission line to couple noise into the computer system. This can be avoided by keeping this ground very short, tying directly to the reference ground plane or ground node, or by insuring that only one conductor is connected to the system and all other signals enter on fiber optics.
 2. *Noise can be avoided by segregating equipment that generates electrical noise from computer circuitry. Relatively small amounts of high frequency electrical noise can disrupt computer operation and cause downtime, loss of function, or spurious equipment operations.*
 3. *When using LAN's, such as Ethernet, and low frequency noise is encountered, the loop may be broken by installing ground isolation devices in the communication network at each node. The ground isolation device will appear as a high pass filter inserted in the communication link. Ensure ground isolation of the communications network at each node.*
 4. *All connections in signal cable should consider possible noise coupling points and should be made carefully with special consideration given to the shield connection. Anytime the shield of a coax cable is broken a coupling path is created for high frequency noise from the outside environment to enter the inside environment of the coax cable shield.*
 5. *The biggest contributor to signal inaccuracy is noise injected into input/output signals. The best way to minimize this noise is through proper grounding and wiring methods of the I/O signal hook-up. IEEE Standard 1050 should be used as a reference on shielding and grounding for instrumentation cables.*
- D. For control and computer/data processing communications protocols that utilize non-isolated systems to transfer data (RS232, RS422, RS423, etc.), the Data Terminal and Communication equipment shall be powered and grounded by the same source as the device providing the signal to prevent ground loops. Peripherals connected to optically isolated communications can be grounded to any grounding system of adequate integrity.³⁰

- E. Facility grounding systems shall be evaluated to ensure the system is adequate for the applicable I&C and/or computer/data processing system and equipment.³¹

Guidance: Large inductive electrical loads cause electrical noise on all conductors in the vicinity and a typical facility ground may have loops that will pick up very large noise voltages. The inadvertent connection of a computer system across such a loop may couple large noise signals into the computer system. To avoid the inadvertent second connection to facility ground, it may be preferable to run a separate ground node for the computer system. This ground node should still tie to the facility ground at a single point for safety reasons. The facility ground system should be evaluated to determine if the network impedance is suitable for a proper ground system. If it is not, then it will be necessary to install a new ground system network that is connected to earth at the same point as the facility ground. Grounding methods should be in accordance with IEEE Standard 142, which complements the NEC.

- F. For I&C and computer/data processing distributed systems, grounding conductor runs over 250 feet shall be avoided. If conductor runs over 250 feet are necessary, a new single point ground node shall be created for all equipment that is located within the 250 foot run limit and connected to the single point earth ground for the facility/system.³²

Guidance: It is possible to treat different system nodes as essentially separate systems as far as grounding is concerned. This adheres to the distributed ground concept in IEEE 1050. Every effort should be made to ground equipment that may communicate in any way to the same earth ground. If more than one piece of equipment is tied to separate earth grounds, the earth currents will create a potential difference between the equipment. A lightning strike or power fault in the vicinity can create hazardous potentials between earth grounds. When distances from a system or equipment to the nearest node become excessive, a new node should be created.

Note: As the frequency increases, the impedance of the ground conductor increases. At 10 Megahertz, the impedance of a typical ground conductor may be in the order of 40,000 ohms and will no longer serve the purpose of providing a common reference point. Where high frequency grounds or connections are required, conductor shape and length must be selected for low inductance (impedance).

- G. *Guidance: The codes, standards and guidelines identified in this section provide grounding practices that should be consistent with most equipment manufacturer requirements. However, these codes, standards and guidelines should be used in conjunction with the manufacturer's computer control and data processing systems grounding recommendations. The manufacturer's grounding specifications should be reviewed for consistency with relevant standards and industry practices. Grounding schemes requiring a dedicated ground conductor routed separately to special earth points would not be acceptable. The I&C and/or computer/data processing system design and installation should be in compliance with the applicable portions of the National Electric Code. Safety takes precedence over potentially conflicting considerations.*

12.0 ADDITIONAL REQUIREMENTS FOR SAFETY-RELATED SYSTEMS (PROGRAMMATIC AND FACILITY)

NOTE: Refer to Section 2.0 for the definition of safety-related systems.

12.1 General

- A. The codes and standards identified within the Task Matrix Table in Section 3.5 contain acceptable methods to satisfy the requirements of this section regarding the design of safety-related systems. Alternative methods can be used as long as the requirements of this section are satisfied. Any implementation methods selected must be justified to ensure that an adequate level of safety commensurate with the identified hazards is achieved.³³
- B. Emergency features shall be provided to include alarms and monitors that alert workers and the public to the existence of unsafe conditions and to record the sequence and severity of an accident.³⁴
- C. Alarms for loss of ventilation or differential pressure shall be provided on primary confinement systems (gloveboxes or hoods).³⁵ *Guidance: Alarms for loss of ventilation or differential pressure should also be considered on secondary confinement systems (rooms).*
- D. The requirements from 29 CFR 1910, Subpart Z, shall be addressed for monitoring and alarms systems for facilities that manage or use specific hazardous materials.³⁶
- E. Alarms shall be provided to annunciate in the event concentrations of radioactive or hazardous materials above specified limit are detected in an effluent stream.³⁷
- F. Adequate instrumentation and controls must be provided to assess system performance and to allow the necessary control of system operation.³⁸
- G. Emergency evacuation annunciation systems must conform to ANSI/ANS N2.3. General communication system installation requirements must be in accordance with NFPA 72, Sections 3-12, 6-3 and 6-4. Section 3-12 describes the minimum requirements for transmission of alarm conditions to building occupants, and Section 6-3 and 6-4 include minimum requirements for audibility above background noise and the use of visual signals, including minimum light intensities.³⁹
- H. The safety functions of instrumentation, control, and alarm systems shall:⁴⁰
 - 1. Provide information on out-of-tolerance conditions/abnormal conditions.
 - 2. Ensure the capability for manual or automatic actuation of safety systems and components.
 - 3. Ensure safety systems have the means to achieve and maintain a fail-safe shutdown condition on demand under normal and abnormal conditions, actuate alarms to reduce public or site-personnel risk, and inform operators of safety actions required and completed (e.g., effluent monitoring components and system).

- I. The design of safety-related instrumentation and control systems must incorporate sufficient independence, redundancy, diversity, and separation to ensure that all safety-related functions associated with such equipment can be performed under postulated accident conditions as identified in the safety analysis. Under all circumstances, ML-1/safety-class instrumentation, controls, and alarms must be designed so that failure of non-safety equipment will not prevent the former from performing their safety functions.⁴¹ *Guidance: Safety-significant components should be evaluated as to the need for redundancy on a case-by-case basis*
- J. Safety-related instrumentation and alarm-system designs must ensure accessibility for inspection, maintenance, calibration, repair, or replacement.⁴²
- K. Safety-related instrumentation, control, and alarm systems must provide the operators sufficient time, information, and control capabilities to perform the following safety functions:⁴³
 - 4. Readily determine the status of critical facility parameters to ensure compliance with the limits specified in the Technical Safety Requirements.
 - 5. Initiate and verify completion of manual safety functions or verify automatic action is initiated and completed.
 - 6. Determine the status of safety systems required to ensure proper prevention of the accident or mitigation of the consequences of postulated accident conditions and/or to safely shut down the facility.
- L. *Guidance: IEEE standards contain design, installation, and testing requirements that should be considered for instrumentation, control, and alarm components without invoking all of the Safety Class 1E requirements. See Section 3.5, National Codes and Standards – Task Matrix, for the relevant codes.*
- M. Safety-related ventilation system designs must provide manual or automatic protective control features as needed to prevent or mitigate an uncontrolled release of radioactive and/or hazardous material to the environment and to minimize the spread of contamination within the facility. Also, inclusion of adequate instrumentation to monitor and assess performance with necessary alarms for annunciation of abnormal or unacceptable operation is required.⁴⁴
- N. *Guidance: The preferred method to prevent or mitigate a safety basis event is to provide automatic protective features with appropriate alarms to indicate the approach to actuation of the automatic feature and monitoring devices to provide accurate indication of the sensed parameter value, etc.*
- O. ML levels and SS and SC are discussed in [LIG230-01-02, Graded Approach for Facility Work](#).

12.2 Installation of Safety-Related Systems⁴⁵

- A. Installations shall conform to instrument location, installation and isometric (if provided) drawings. These documents shall establish the installation design requirements for ML-1 and/or Safety Class and ML-2 and/or Safety Significant instruments and their sensing lines, with regard to their safety function, postulated health hazard and their protection against failure.⁴⁶

- B. ML-1/Safety Class redundant instruments, instrument tubing, and piping (sensing lines) shall be routed and/or protected to withstand the credible effects both during and following design bases accidents for which the instruments/systems are required to perform.⁴⁷
- C. Separation of redundant ML-1/Safety Class or redundant (as determined by safety analysis) ML-2/Safety Significant instrument shall be achieved by the use of structures, distance, barriers, or any combination thereof. Any deviation from these methods of separation must be submitted for approval.⁴⁸
- D. For technical requirements for ML-1 and/or Safety Class and ML-2 and/or Safety Significant tubing and piping systems, see Mechanical Chapter 6.
- E. Redundant ML-1/Safety Class and redundant (as determined by safety analysis) ML-2/Safety Significant instrument sensing lines shall be routed and protected so that the failure of one redundant system will not disable equipment essential to the operation of the other redundant system(s). Sensing lines of one channel shall not crossover or come in contact with equipment of another redundant channel, whether it is in the same or another functional loop of another channel.⁴⁹
- F. ML-1/Safety Class and ML-2/Safety Significant wiring, sensing lines, and mechanical signal lines shall not be routed where vibration, abnormal heat, or stress could affect performance.⁵⁰
- G. When locating safety instruments on racks or in cabinets, care must be given to assure that no two redundant instruments are mounted on the same rack or in the same cabinet.⁵¹
- H. The minimum separation between instrument sensing lines of redundant channels shall be at least 46 cm (18 inches) in air in both horizontal and vertical directions in non-missile or jet impingement areas. The 46 cm (18 inches) minimum spacing required between the redundant channels shall be maintained from its starting point at the root valve to the vicinity of the instrument. If this separation is not possible, Engineering shall be consulted to determine if a suitable barrier should be used. A barrier may be equipment, structural steel shapes, building structures such as walls, ceilings, floors and shield walls. When a barrier is used, it shall extend at least 2.5 cm (1 inch) beyond the line of sight between the two redundant channel sensing lines. Where potential missiles can be identified, additional separation, barriers and/or missile shields may be necessary. Missile shields may be structural steel shapes such as plate, channel and angle, covered tray or pipe guards.⁵²
- I. Supports, brackets, clips or hangers shall not be fastened to the sensing lines or their supports for the purpose of supporting other equipment, cables, etc., without specific approval.⁵³
- J. Where instrument sensing lines of more than one channel of a redundant set penetrate a wall or floor, the redundant sensing lines shall be routed through separate penetrations and separated by a minimum distance of 46 cm (18 inches). If the use of separate penetrations is not feasible, approval is required to use a common penetration. The use of a common penetration may require the design of:⁵⁴
 - 1. A Suitable barrier, such as a guard pipe, to protect instrument sensing lines in one channel or division from postulated effects of a failure of the other channels or divisions.

2. A missile shield, to be installed around the lines until a minimum separation distance of 46 cm (18 inches) is achieved between the different redundant sensing lines.
- K. Instrumentation and sensing lines shall be easily identified and distinctly labeled as ML-1/Safety Class or ML-2/Safety Significant. Each instrument sensing line, as a minimum, shall be tagged at its process line root valve connection, at the instrument, and at any point in between where the sensing line passes through a wall or a floor (on both sides of such penetrations).⁵⁵
- L. Barriers used to protect instrumentation (as determined by safety analysis) shall be identified in the field, to prevent inadvertent degradation of this protection.⁵⁶
- M. To prevent the loss of both parts of a redundant set of instruments, separate process pipe connections with sufficient separation shall be used wherever possible.⁵⁷
1. When a single process connection must be used, the system shall be designed for a “safe” trip action of the channel upon tap or sensing line breakage.
 2. The single process connection shall be protected from credible sources of damage and separation of the redundant sensing lines shall be achieved as close as possible to the process connection.

12.3 Application of ISA 84.01 for LANL Non-Reactor Facilities⁵⁸

- A. ANSI/ISA 84.01 shall be applied in the design, installation and testing of nuclear Safety Significant instrumented systems and non-nuclear instrumented systems that would be considered SS using the definition in Section 2.0. The standard shall also be applied to safety-related ML-2 instrumented systems. The following constitute specific clarifications, modifications, substitutions, additions, or deletions to the identified sections of ISA 84.01, for use in LANL non-reactor facilities. Those not specifically referenced are deemed appropriate as written, except for word substitutions.
- B. Word Substitutions:
1. “Safety Significant Instrumented System” is substituted for “Safety Instrumented System” in ISA 84.01.
 2. “SSIS” is substituted for “SIS” in ISA 84.01.
 3. “Facility is substituted for “unit” in ISA 84.01.
- C. The first sentence of ISA 84.01, Scope Clause 1, is revised as follows to clarify that the standard is applicable to Safety Significant or hazardous process systems in LANL non-reactor facilities:
- “This standard addresses Electrical/Electronic/Programmable Electronic Systems (E/E/PES), associated sensors, logic devices, final elements, and interfaces used in LANL non-reactor nuclear and non-nuclear facilities with Safety Significant or 29 CFR 1910.119 designated process safety instrumented systems.”

- D. ISA 84.01, Section 1.2 Exclusions, Item 1.2.4, is revised as follows to clarify that the standard is applicable to non-reactor nuclear facilities:

“This standard does not address the codes, regulations, and other requirements that apply only to the Nuclear Power Industry.”
- E. ISA 84.01, Section 1.2 Exclusions, Item 1.2.14, is deleted since operation action, as part of a SSIS, would be covered by the standard when operator action is justified by qualification and training and there is sufficient time for the operator to respond to an alarm.
- F. ISA 84.01, Section 2.2 Existing systems, is deleted. The Code of Record governs the design of existing facilities. When modifications are made the engineer/designer determines whether to use the existing Code of Record or current codes and standards. The Code of Record governs the design for the replacement SSCs.
- G. The following acronyms shall be added to ISA 84.01, Section 3.2 Acronyms:
 - 1. SSC: Systems, Structures and Components
 - 2. SSIS: Safety Significant Instrumented System
- H. ISA 84.01, Section 8.0 shall be implemented using LANL policies and procedures for the subject areas of Installation, Commissioning and Pre-Startup acceptance test, SSIS operation and maintenance, SSIS Management of Change, and Decommissioning.

12.4 Application of IEEE 384-1992 for LANL Non-Reactor Facilities⁵⁹

- A. IEEE 384-1992 shall be used to satisfy the requirements of DOE O 420.1 unless an alternative method is justified in the Design Documents. The following constitute specific clarifications, modifications, substitutions, additions, or deletions to the identified sections of the standard, for use in LANL non-reactor facilities. Those not specifically referenced are deemed appropriate as written, except for word substitutions.
- B. Word Substitutions:
 - 3. “Control room” is substituted for “main control room” and/or “central control room” in IEEE 384-1992, since a control room in a non-reactor facility serves the same function as the main control room in a nuclear power generating station.
 - 4. “Emergency” is substituted for “Standby” in IEEE 384-1992.
 - 5. “Facility” is substituted for “unit” and/or “station” in IEEE 384-1992.
 - 6. “Non-reactor facility” is substituted for “nuclear power generating station” in IEEE 384-1992.
- C. IEEE 384-1992, Section 2 Purpose, is revised as follows to add DOE Order 420.1, since the order defines the facility design criteria:

“This standard establishes the guidance for implementation of the independence criteria of DOE Order 420.1, IEEE 603 and IEEE Std 308-1991. In addition, this standard provides criteria for implementation of independence requirements for safe shutdown systems.”

- D. *Guidance: IEEE 384-1992, Section 3 References, has a list of other standards that are to be used with IEEE 384-1992. All standards referenced by IEEE 384-1992 should be used only as information to be considered during the design of a facility or a project.*
- E. The following applies to IEEE 384-1992, Section 4 Definitions:
1. The definition of “Class 1E” is deleted from the section.
 2. The definition of “emergency power” is added as follows to replace “standby power”, since the term “standby power” as it applies to LANL non-reactor facilities is used to supply non-safety systems as described in NFPA 70, NFPA 110, and IEEE 446:
 “The power supply that is provided to ML-1/Safety Class equipment and/or ML-1/Safety Class systems to allow them to maintain their safety functions during periods of partial or total failure of the preferred power system.”
 3. The definition of “exposure fire” is added as follows from 10 CFR 50, Appendix R, to clarify the independence requirements for safety shutdown systems that have been added as criteria:
 “A fire in a given area that involves either in situ or transient combustibles and is external to any structures, systems or components located in or adjacent to that same area. The effects of such fire (e.g., smoke, heat, or ignition) can adversely affect those structures, systems, or components important to safety.”
 4. The definition of “safe shutdown” is added as follows to establish the meaning of safe shutdown for a non-reactor nuclear facility:
 “Safe shutdown in a non-reactor nuclear facility is a shutdown of a process with (1) the reactivity (nuclear or chemical) of the process kept to a margin below criticality (prevent accidental nuclear criticality) consistent with the facility technical specifications, (2) systems, structures, and components necessary to maintain this condition operating within their design limits, and (3) components and systems necessary to keep offsite doses within prescribed limits operating properly.”
- F. The following applies to IEEE 384-1992, Section 5 General Independence Criteria:
1. The “Note” at the end of Section 5.5.2, Criteria (Associated Circuits), is revised as follows to delete the reference to unit generators:
 “Preferred power supply circuits from the transmission network that become associated circuits solely by their connection to the ML-1/Safety Class distribution system input terminals are exempt from the requirements for associated circuits.”
 2. The following sentence is added to Section 5.10.2, Fire, to provide a clarification of fire protection for ML-1/Safety Class systems to prevent the over design of ML-1/Safety Class systems that are not required for safe shutdown:
 “ML-1/Safety Class systems, not located in fire hazard areas, used to mitigate the consequences of design basis events but not required for safe shutdown, may be lost to a single exposure fire.”

G. The following applies to IEEE 384-1992, Section 6 Specific Separation Criteria:

1. The following Note is added to the end of Section 6.1.1.2, Minimum Separation Distances (Cable and Raceways). The reduced separation allowed by considering the identified types of cables as enclosed conduit for instrument and control cables has been approved and used in the commercial nuclear industry.

“Mineral Insulated (MI) and Aluminum Sheathed (ALS) cable can be considered as enclosed raceways for instrument and control cables only.”

2. The term “standby generating unit” is substituted with the term “emergency generating unit” wherever it is used in Section 6.2, Standby Power Supply, to stay consistent with the general substitution of “emergency” for “standby”.

H. The following represents additional content added to IEEE 384-1992, Section 7.2, under the Heading, “Non-Safety Class Power Supplying ML-1/Safety Class Equipment”.

1. Electrical isolation of Non-Safety Class power circuits from ML-1/Safety Class components should be achieved by ML-1/Safety Class isolation devices applied to interconnections of the Non-Safety Class power circuits and the ML-1/Safety Class component/function (See Fig. 9 of IEEE 384-1992).
2. Sections 7.1.2 and 7.2.2 of IEEE 384-1992 provide general information for protective devices for this particular type of interconnection.

However, for this interconnection a device is considered an electrical isolation device for power, and instrumentation and control circuits if it is applied so that (a) the maximum credible voltage or current transient applied to the device’s ML-1/Safety Class side will not degrade the operation of the circuit connected to the device’s non-safety side below an acceptable level; and (b) shorts, grounds, or open circuits occurring in the ML-1/Safety Class side will not degrade the circuit connected to the device’s non-safety side below an acceptable level.

The highest voltage to which the isolation device ML-1/Safety Class side is exposed should determine the minimum voltage level that the device should withstand across the ML-1/Safety Class side terminals, and between the ML-1/Safety Class side terminals and ground. Transient voltages that may appear in the ML-1/Safety Class and Non-Safety Class sides must also be considered.

The separation of the wiring at the input and output terminals of the isolation device may be less than 1 in (2.5 cm) as required in 6.6.2 of IEEE 384-1992 provided that it is not less than the distance between input and output terminals.

Minimum separation requirements do not apply for wiring and components within the isolation device; however, separation should be provided wherever practicable.

The capability of the device to perform its isolation function should be demonstrated by qualification test. The test should consider the levels and duration of the fault current on the ML-1/Safety Class side.

3. When the requirements of Items 1 and 2 above are met, the following devices may be used as acceptable isolation devices for instrumentation and control circuits:
 - a. Amplifiers
 - b. Control switches

- c. Current transformers
- d. Fiber optic couplers
- e. Photo-optical couplers
- f. Relays
- g. Transducers
- h. Power packs
- i. Circuit breakers
- j. Input current limiters

Note: In using contact-to-contact isolation, consideration should be given to the effect on independence that may occur from welding of contact.

- 4. When the requirements of Items 1 and 2 above are met, a fuse may be used as an isolation device (except between redundant divisions) if the following additional criteria are met. The requirements have been developed because of the methodology used to classify a component or a component's function. A component may be classified as ML-1/Safety Class, but does not rely on electric power to perform its safety function. The electric power is present only for operational requirements. Therefore, the power may be obtained from a Non-Safety Class source if proper circuit protection is provided.
 - k. Fuses should provide the design overcurrent protection capability for the life of the fuse.
 - l. The fuse time-overcurrent trip characteristic for all circuit faults should cause the fuse to open prior to the initiation of an opening of any upstream interrupting device.
 - m. The power source should supply the necessary fault current to ensure the proper coordination without loss of function of other Non-Safety loads.

- I. The following represents additional content added to IEEE 384-1992, under the Section Heading, "ML-1/Safety Class Safe Shutdown Cables and Equipment".
 - 1. General: ML-1/Safety Class safe shutdown cables and equipment should comply with the requirements of previous sections of this document and the following additional requirements.
 - 2. The independence of redundant ML-1/Safety Class safe shutdown cables and equipment should be maintained for a single postulated exposure fire.
 - 3. A single exposure fire should be postulated in those areas of the facility which contain cables or equipment necessary to provide safe shutdown capability in the event of fire.
 - 4. An exposure fire should be postulated to occur regardless of whether or not the area contains ignition sources or combustible materials.
 - 5. Exposure fires should not be postulated concurrent with non-fire related failures in ML-1/Safety Class systems, design basis events, or natural phenomena (for example, earthquakes, tornado).

6. The independence of ML-1/Safety Class safe shutdown systems, structures, and components should be such that a single postulated exposure fire should not defeat the safe shutdown function.
7. Redundant ML-1/Safety Class cables and equipment required for safe shutdown should be located in different fire areas. The area boundaries should meet the requirements of section 6.1.8.2 of IEEE 384-1992.
8. When redundant safe shutdown cables and equipment are located within the same fire area, one of the following requirements must be met:
 - a. Redundant ML-1/Safety Class cables and equipment required for safe shutdown should be separated from each other by a 3-hour fire barrier. Structural steel forming a part of or supporting such fire barriers should be protected to provide fire resistance equivalent to that required of the barrier.
 - b. Separation of cables and equipment of redundant divisions by a horizontal distance of more than 20 feet with no intervening combustibles or fire hazards. In addition, fire detectors and an automatic fire suppression system should be installed in the fire area.
 - c. Enclosure of cables and equipment of one redundant division in a fire barrier having a 1-hour rating. In addition fire detectors and an automatic fire suppression system should be installed in the fire area.

ENDNOTES:

1. LANL LIR 220-03-01.1, "LANL Engineering Standards Manual" is the implementation requirement document for this manual. Refer to Sections 2.0 and 3.0 for statements of the purpose, scope and applicability of the ESM.
2. Replacement value determined using recognized cost estimating procedures and a national material and labor cost database.
3. This is more restrictive than the UBC. Over time this requirement will bring about upgrades to the underlying I&C systems in facilities. This percentage was accepted by the TRB per Minutes from the Facility Engineering Manual Technical Review Board meeting on 7/19/00. Fifty percent is also used in Chapter 7; in the 2001 Santa Fe County Urban Wildland Interface Code for use of fire resistant materials in renovations; and for the total luminaire replacement requirement in ASHRAE/IESNA 90.1-2001, Section 4.1.2.2.5.
4. The Facility Engineering Manual (FEM) LIR was re-titled LANL Engineering Manual in June 2001 to allow inclusion of programmatic requirements. This was primarily to support TA-55 Type A corrective actions relating to design and installation of compression fittings, Teflon, and gloveboxes. [Type A Accident Investigation of the March 16, 2000 Plutonium-238 Multiple Intake Event at the Plutonium Facility Los Alamos National Laboratory New Mexico](http://tis.eh.doe.gov/oversight/reports/accidents/typea/0003lanl/html/) dated 7/2000 at <http://tis.eh.doe.gov/oversight/reports/accidents/typea/0003lanl/html/>. It was also in response to the January 2001 clarification of 10CFR830 scope to include all activities affecting nuclear safety. The identification of these and only these specific mechanical requirements for programs was directed in the 11/20/01 LANL Operations Working Group meeting until such time as programmatic involvement in the LEM upkeep was put in place.

Looking forward: As the name implies, the FEM addressed site-specific LANL requirements applicable to facility systems. Any further extension or adaptation of such lab-wide requirements to programmatic and experimental installations must provide flexible and cost-effective approaches that will ensure protection for the environment, the safety of LANL workers, and the protection of the equipment and facilities that they use and occupy. Several different situations seem apparent:

- A. Some permanently installed programmatic components (e.g. glove boxes and fume hoods) so closely resemble "facility" equipment that coverage by and compliance with the LEM makes sense from the standpoint of standardized design, construction, operations, and maintenance.
- B. Some programmatic installations (e.g. control wiring and components) are at least partially addressed in national standards or DOE publications and addressed by the I&C chapter to varying extents. Chapter-maintaining personnel plan over time to identify these, collect information, and document in the LEM site-specific recommended practices. Requirements would only be added with the concurrence of affected programs.
- C. Some programmatic equipment is set-up and used for only a short time or is intentionally destroyed in the course of the experiment. Clearly it is not cost-effective to require that such installations comply with the LEM; however, facilities must be protected, and the safety of workers must be assured. As a starting point, national code and standard requirements for temporary installations could be sought out and applied to such installations.
- D. Some very specialized programmatic equipment is clearly far outside the scope of any national standards. Allowing only authorized and qualified technicians using approved procedures described in written SOPs or HCPs to use this equipment controls the risks. The LEM may be applicable up to an identifiable point of demarcation such as a support system boundary.

5. [LIR 220-03-01.1](#), LANL Engineering Standards Manual, empowers the POCs as the Authority Having Jurisdiction for their discipline chapter and related national codes and standards, with rare exceptions.
6. NEC Sections 90.7, 110.2, and 110.3.
7. Part of Appendix G of the University of California/DOE Contract.
8. [LIR 220-03-01.1](#), LANL Engineering Standards Manual.
9. The National Codes and Standards given in the Task Matrix are established for compliance with DOE O 420.1, "Facility Safety". The majority of the standards are taken directly from DOE G 420.1-1, "Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria Guide for use with DOE O 420.1 Facility Safety". The codes are identified in the tables of DOE G 420.1-1 and ensure compliance with the requirements of DOE O 420.1 for Safety Significant and Safety Class I&C related systems. Additional standards have been added that provide safety-related I&C system design, quality assurance and implementation requirements and are given to supplement those standards directly referenced within DOE G 420.1-1. The required compliance with additional national codes and standards is also established at SRS through the SRS Engineering Standards Manual WSRC-TM-95-1, "Introduction Attachment 1, National Codes and Standards for Engineering/Design Tasks Matrix, 9/99".
10. The standard for the design, installation, operation, maintenance, start up and periodic functional testing, and management of safety instrumented systems. The standard promotes a risk-informed performance-based methodology for the life cycle management of safety systems. The methodology was applied at SRS to provide a graded approach to the design of Safety Significant Instrumented Systems (SSISs) in non-reactor nuclear process facilities, based on the unmitigated risk (consequence and frequency) of the safety significant event. (Reference: WSRC-MS-2001-00404 Rev 0, "Implementing ISA S84.01 at a Department of Energy Site, Sossman and Suttinger").

The application of ISA 84.01 is a result of several reviews conducted by the Defense Nuclear Facilities Safety Board (DNFSB) of safety significant instrumentation and control systems. These reviews found that some systems did not meet industry standards for reliability. DNFSB letters dated February 7, 2000 and March 30, 2000 addressed these problems and identified the ISA 84.01 standard for use by DOE as a design guideline for safety significant instrumented systems. Per the recommendation of the DNFSB, this standard has been adopted at several DOE sites. (Reference: Defense Nuclear Facilities Safety Board Eleventh Annual Report to Congress, February 2001).
11. Identified for use in 6430.1A, Section 1300-6.5.5.
12. Taken from ASME AG-1-1997, "Code on Nuclear Air and Gas Treatment" – Article IA-4120, and supplemented by SRS Standards, Guides, and Engineering Manual E7. The listing identifies the necessary input that is required for the selection of appropriate I&C devices.
13. LIR240-01-01.2, "Facility Configuration Management" requires the development of a System Design Description for SSCs classified as ML-1/SS, ML-2/SC, or those ML-3/General System SSCs that provide a mission critical, defense in depth, or worker safety function or whose failure may impact operation of safety related SSCs.
14. A System Design Description is required for the design and configuration of ML-1/SS and ML-2/SC systems in accordance with LIR240-01-01.2, "Facility Configuration Management". Requirement established from DOE-STD-3024 and supplemented by SRS Engineering Manual E7.

15. The list establishes the essential content for a System Design Description and was developed by SRS in accordance with DOE-STD-3024, "Content of System Design Descriptions". The required content is mandated by SRS through the SRS Engineering Manual E7.
16. The document listing is taken from ASME AG-1-1997, "Code of Nuclear Air and Gas Treatment", and identifies the types of I&C documentation that should be requested from the manufacturer.
17. Memo from Lab Counsel to Tobin Oruch, 7/19/01.
18. Sustainable (energy-efficient) building design is a requirement identified through Department of Energy directives DOE O 430.2A, "Departmental Energies and Utilities Management", and DOE O 413.3, "Program and Project Management for the Acquisition of Capital Assets". ASHRAE 90.1 provides the minimum requirements for the energy-efficient design of buildings that will satisfy the DOE sustainable building design requirements.
19. Pays back in energy savings and supports sustainable design requirements in DOE Order 420.2X, DOE 413.3, and 10CFR435.
20. 1997 IAPMO UMC, Section 305.
21. DOE-HDBK-1140, "Human Factors / Ergonomics Handbook for the Design for Ease of Maintenance", Section 4.9.3.6, identifies a maximum usage height of 12 feet for a painter's type stepladder. For Safety-Related systems this represents the minimum height for ease of surveillance and maintainability given the potential apparatus available for the performance activities.
22. [LIR/LIG 402-100-01](#), Signs, Labels, and Tags; and 1997 IAPMO UPC, Section 601.2.
23. The requirements identified within the Environmental Considerations section are "Good Engineering Practice" and must be established for Safety-Related systems to ensure that the environment in which the systems will be placed is conducive to the performance attributes of the selected I&C components. DOE G 420.1-1, Section 5.1.1.3, establishes the requirement for Environmental Qualification as deemed necessary to ensure reliable performance of a safety system under those conditions and events for which it is intended.

The requirements and guidance within the section are developed through several standards. ASME AG-1, "Code on Nuclear Air and Gas Treatment", Article IA-4000 – Design Considerations, requires the identification of environmental conditions for safety-related systems. Additional requirements and guidance were developed through several standards that identify environmental conditions that could adversely impact the operability of I&C equipment. These standards establish methods to recognize and classify such environmental conditions. The standards are provided as follows:

- ISA-71.01, "Environmental Conditions for Process Measurement and Control Systems: Temperature and Humidity"
- ISA-71.02, "Environmental Conditions for Process Measurement and Control Systems: Power"
- ISA-71.03, "Environmental Conditions for Process Measurement and Control Systems: Mechanical Influences"
- ISA-71.04, "Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants"
- IEEE 1-2000, "Recommended Practice – General Principles for Temperature Limits in the Rating of Electrical Equipment and for the Evaluation of Electrical Insulation"
- IEEE-1159, "Recommended practice for Monitoring Electric Power Quality"

- IEEE-1100, “Recommended Practice for Powering and Grounding Electronic Equipment IEEE Emerald Book”.
- 24. From NUREG-0700, “Human-System Interface Design Review Guidelines”, and IEEE-1023, “IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations”. DOE G 420.1-1, Section 3.6, identifies these standards as recommended sources for Human Factors Engineering principles and criteria.
- 25. Established from NUREG-0700, “Human-System Interface Design Review Guidelines”, Section 13.1.5 – Protecting Equipment and Components from Hazards.
- 26. Established from NUREG-0700, “Human-System Interface Design Review Guidelines”, Section 13.1.5 – Protecting Equipment and Components from Hazards.
- 27. Taken from SRS Engineering Standards Manual WSRC-TM-95-1, “Color Conventions for Process Displays”, in accordance with ANSI / ISA 5.5-1985, “Graphic Symbols for Process Displays”.
- 28. The color convention table is taken from NUREG-0700, 1997, Rev. 1, Vol. 1, “Guidelines for Control Room Design Reviews”, and ANSI / ISA 5.5-1985, “Graphic Symbols for Process Displays”.
- 29. Established from NFPA 70, Article 250 – Grounding, Section 250.4 and IEEE 1050, “Guide for Instrumentation and Control Equipment Grounding in Generating Stations”, Section 5.0 – I&C System Grounding.
- 30. Established from IEEE 1100, “IEEE Recommended Practice for Powering and Grounding Electronic Equipment”, Chapter 9 – Telecommunications and Distributed Computing, Section 9.11.2 – Grounding.
- 31. The requirement is deemed “Good Engineering Practice” and is established to ensure that the integrity of the facility grounding system is adequate for proper system operation. An inspection is considered necessary to ensure compliance with NFPA 70.
- 32. The requirement is established to preclude the installation of a ground conductor that would not provide an effective low-impedance current signal reference. Refer to IEEE 1050, “Guide for Instrumentation and Control Equipment Grounding in Generating Stations”, Section 5.2.2 – Ground Conductor Lengths. For Single-point grounding refer to IEEE 1100, “IEEE Recommended Practice for Power and Grounding Electronic Equipment”, Chapter 8 – Grounding Consideration, Section 8.5.4.5 – Single-point and Multi-point Grounding.
- 33. For compliance with DOE O 420.1A
- 34. From DOE G 420.1-1, Section 2.3 – Defense in Depth
- 35. From DOE G 420.1-1, Section 4.2.3 – Special Considerations and Good Engineering Practices
- 36. From DOE G 420.1-1, Section 4.3.3 – General Application
- 37. From DOE G 420.1-1, Section 4.4.2 – Special Considerations and Good Engineering Practices
- 38. From DOE G 420.1-1, Section 4.4.2 – Special Considerations and Good Engineering Practices
- 39. From DOE G 420.1-1, Section 4.7.3 – General Application
- 40. From DOE G 420.1-1, Section 5.2.4 – Instrumentation, Control, and Alarm Systems
- 41. From DOE G 420.1-1, Section 5.2.4 – Instrumentation, Control, and Alarm Systems
- 42. From DOE G 420.1-1, Section 5.2.4 – Instrumentation, Control, and Alarm Systems

43. From DOE G 420.1-1, Section 5.2.4 – Instrumentation, Control, and Alarm Systems
44. From DOE G 420.1-1, Section 5.2.2.1 – Ventilation
45. Taken from SRS Engineering Manual WSRC-TM-95-58, “Mechanical Installation of Safety Class and Safety Significant Instrumentation”, for compliance with DOE Order 420.1A.
46. IEEE 336, “IEEE Standard Installation, Inspection, and Testing Requirements for Power, Instrumentation, and Control Equipment at Nuclear Facilities”.
47. IEEE 384, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits”.
48. IEEE 384, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits”.
49. IEEE 384, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits”.
50. ISA 67.02.01, “Nuclear Safety-Related Instrument Sensing Line Piping and Tubing Standard for Use in Nuclear Power Plants”.
51. IEEE 384, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits”.
52. ISA 67.01.01, “Transducer and Transmitter Installation for Nuclear Safety Applications”.
53. ISA 67.02.01, “Nuclear Safety-Related Instrument Sensing Line Piping and Tubing Standard for Use in Nuclear Power Plants”.
54. ISA 67.01.01, “Transducer and Transmitter Installation for Nuclear Safety Applications” and ISA 67.02.01, “Nuclear Safety-Related Instrument Sensing Line Piping and Tubing Standard for Use in Nuclear Power Plants”.
55. ISA 67.02.01, “Nuclear Safety-Related Instrument Sensing Line Piping and Tubing Standard for Use in Nuclear Power Plants”.
56. ISA 67.01.01, “Transducer and Transmitter Installation for Nuclear Safety Applications”.
57. ISA 67.02.01, “Nuclear Safety-Related Instrument Sensing Line Piping and Tubing Standard for Use in Nuclear Power Plants”.
58. Provides the requirement for implementation of ISA S84.01-1996, “Application of Safety Instrumented Systems for the Process Industries”, for ML-2 / Safety Significant Systems and how the standard is interpreted for application within DOE non-reactor facilities.
59. Provides an interpretation of how IEEE 384-1992, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits”, should be applied within DOE non-reactor facilities.

ATTACHMENT 1

DESIGN GUIDANCE FOR INSTRUMENTED SYSTEMS USED IN SAFETY SIGNIFICANT AND HAZARDOUS PROCESSES (PROGRAMMATIC AND FACILITY)

TABLE OF CONTENTS

1.0	PURPOSE	2
2.0	SCOPE	2
3.0	ACRONYMS AND DEFINITIONS	2
4.0	SYSTEM ARCHITECTURE	5
5.0	SYSTEM BOUNDARIES / CONSTRAINTS	6
6.0	SSIS LIFE CYCLE.....	6
7.0	DESIGN INPUTS.....	8
8.0	DESIGN CRITERIA	9
9.0	DESIGN VERIFICATION	11
10.0	BACKFIT ANALYSIS	11
	APPENDIX A: SAFETY INTEGRITY LEVEL ASSIGNMENT METHODOLOGY.....	12
	APPENDIX B: SAFETY SIGNIFICANT INSTRUMENTED SYSTEM CHECKLIST.....	24

RECORD OF REVISIONS

Rev	Date	Description	POC	OIC
0	10/--/03	Initial issue	Mel Burnett, <i>FWO-DECS</i>	Gurinder Grewal, <i>FWO-DECS</i>

1.0 PURPOSE

This attachment provides guidance for the development of performance attributes and design criteria for electrical/electronic/and programmable electronic systems classified as safety significant or protection layers for hazardous processes. The development of design criteria for these systems is based on the ANSI/ISA 84.01 Standard. ISA 84.01 provides a performance based graded approach to the design of safety instrumented systems.

2.0 SCOPE

The guidance presented in this attachment applies only to systems that (1) are identified as a nuclear Safety Significant system, a non-nuclear system that would be considered Safety Significant using the definition in Section 3.0 below, or a safety-related ML-2 system, and (2) require instrumented systems to perform the safety function. Operator actions in response to process alarms that place a process in a safe state in order to prevent or mitigate a safety significant risk are covered within this attachment. The attachment does not cover the methods or procedures to be used to conduct a hazard analysis, perform a risk assessment, develop a risk/consequence based matrix, identify functional classifications, or identify means to be used to prevent and/or mitigate any hazards identified.

3.0 ACRONYMS AND DEFINITIONS

3.1 ACRONYMS

AC – Administrative Control

ANS – American Nuclear Society

BPCS – Basic Process Control System

DCS – Distributed Control System

FM – Factory Mutual

IPL – Independent Protection Layer

ISA – Instrument Society of America

LOC – Level of Control

LOPA – Layer of Protection Analysis

ML – Management Level

PFD – Probability of Failure on Demand

PHA – Process Hazards Analysis

RFI – Radio Frequency Interference

RRF – Risk Reduction Factor

SIL – Safety Integrity Level

SIS – Safety Instrumented System

SS – Safety Significant

SSCs – Systems, Structures and Components

SSIS – Safety Significant Instrumented System.

TSR – Technical Safety Requirement

TUV – Technischer Überwachungs-Verein (Technical Inspection Association of Germany)

3.2 DEFINITIONS

Administrative Control – Provision relating to organization and management, procedures, record keeping, assessment, and reporting necessary to ensure the safe operation of the facility.

Analytical Limit – Limit of a measured or calculated process parameter established by the safety or hazards analysis to ensure that a safety limit is not exceeded.

Backfit Analysis – The process by which an existing SSC is evaluated to determine if it is adequate to perform its upgraded safety function in terms of newly established requirements and safety analyses. Backfit consists of a design assessment and if needed a cost benefit assessment.

Basic Process Control System (BPCS) – A system that responds to the input signals from the process, its associated equipment, other programmable systems and/or an operator and generates outputs signals causing the process and its associated equipment to operate in the desired manner but does not perform any safety instrumented functions.

Common Cause Failure – A single event that causes failure in multiple elements of a system. The initiating event may be either internal or external to the system.

Design Agency – The organization performing the detailed design and analysis of a project or modification.

Design Authority – The person or group responsible for the final acceptability of and changes to the design of a system or component and its technical baseline (typically the manager of engineering).

Fail-Dangerous Fault – A failure in a system or component that will result in the system/component not performing its safety function.

Fail-Safe – Fail-safe means that on loss of motive force (electrical power, air supply, hydraulics, etc.) the system will go to a safe state and remain in this safe state.

Functional Classification – A graded classification system used to determine minimum requirements for SSCs. The Functional Classifications in order of precedence are ML-1 or Safety Class, ML-2 or Safety Significant, and ML-3 or General Service.

Independent Protection Layer (IPL) – A system, structure, component, or administrative control that acts to prevent or mitigate a safety significant hazardous event. Independent Protection Layers are sufficiently independent so that the failure of one IPL will not cause the failure of another IPL that is credited with preventing or mitigating the same event.

Layer of Protection Analysis (LOPA) – A Layer of Protection Analysis is a variation of event tree analysis where only two outcomes are considered. The possible outcomes are either failure (PFD) or successful operation.

Level of Control (LOC) – One or more structures, systems, components, administrative controls, or inherent features (e.g. chemical properties, gravity, physical constants, underground location) which can be readily expected to act to prevent or mitigate a hazardous event.

Management Level 2 (ML-2) – Selective application of applicable codes, standards, procedural controls, verification activities, documentation requirements, and formalized maintenance program (i.e., certain elements may require extensive controls, while others may only require limited control measures). Could include facility work that may require independent review, management approval, and verification of design outputs, surveillance during procurement, fabrication, installation, assembly, and construction.

Probability of Failure on Demand (PFD) – A value that indicates the probability of a system failing to respond to an event for which it is designed. The average probability of a system failing to respond to a demand in a specified time interval is referred to as PFDavg.

Risk Reduction Factor (RRF) – The inverse of Probability of Failure on Demand (1/PFD). The risk reduction factor is a numeric value identifying the amount of reduction or lessening of the likelihood of an event occurring.

Safety-Related – A term meaning safety class, safety significant, and those ML-1 and ML-2 SSCs that could potentially impact public or worker safety or the environment in the same way as safety class or safety significant systems respectively.

Safety Significant (SS) – Structures, Systems, and Components that are not designated as Safety-Class SSCs but whose preventive or mitigative function is a major contributor to defense in depth and/or worker safety as determined from safety analyses. [10 CFR 830]

As a general rule of thumb, Safety-Significant SSC designations based on worker safety are limited to those Systems, Structures, or Components whose failure is estimated to result in a prompt worker fatality or serious injuries or significant radiological or chemical exposures to workers. The term, serious injuries, as used in this definition, refers to medical treatment for immediately life-threatening or permanently disabling injuries (e.g., loss of eye, loss of limb).

Safety Significant Functions – SS functions are those functions that have been classified as either SS or ML-2 through the hazards analysis and graded approach.

Safety Significant Hazardous Event – An event involving a source of danger (i.e. material, energy source, or operation) with the potential to cause illness, injury, or death to personnel or damage to a facility or to the environment that has a functional classification of SS or ML-2.

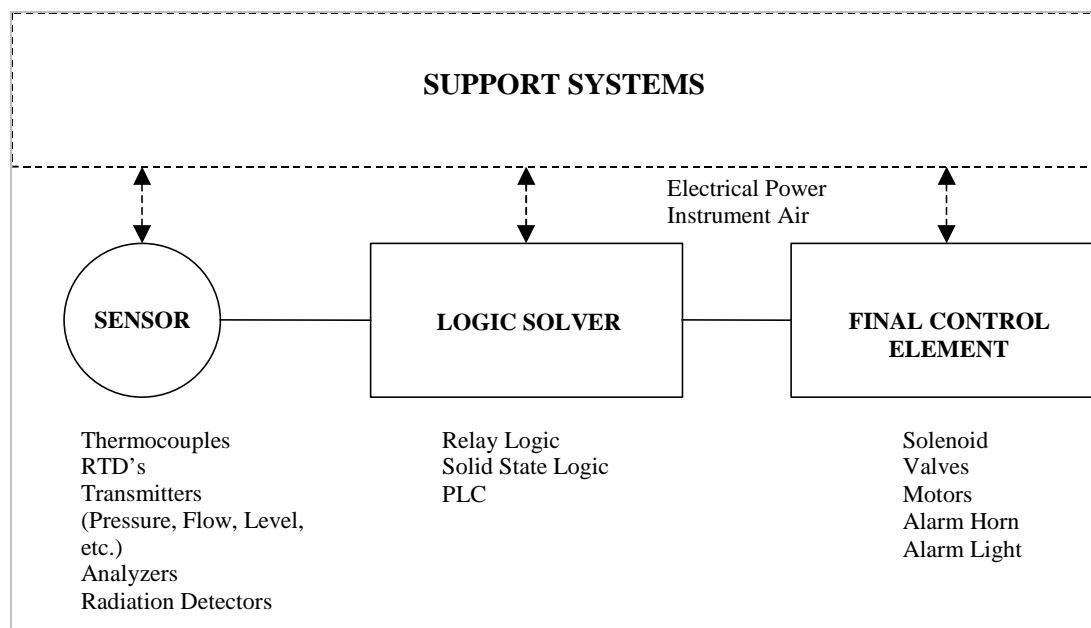
Safety Significant Instrumented System (SSIS) – An SS system, a safety-related ML-2 system, or a 29 CFR 1910.119 hazardous process independent protection layer that requires instrumentation, logic devices and final control elements to monitor and detect an SS/ML-2 event, and which will result in automatic or operator action that will bring the facility or process system to a safe state.

TUV – A German based certification organization that provides certification services to manufacturers of safety instrumentation and safety systems.

4.0 SYSTEM ARCHITECTURE

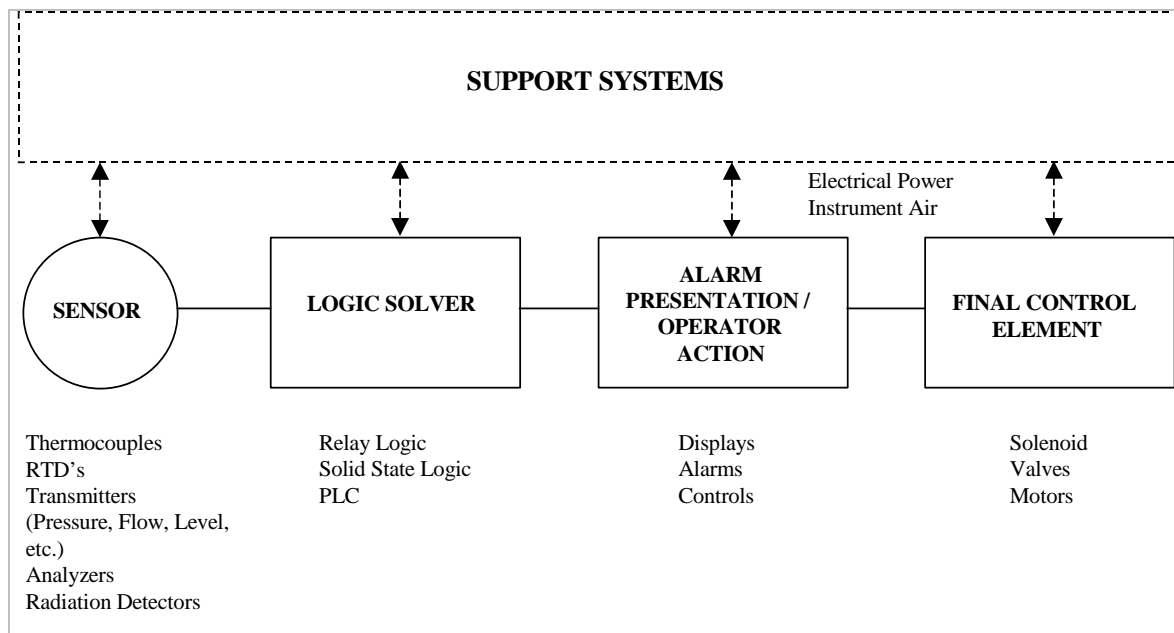
- A. A Safety Significant Instrumented System (SSIS) generally consists of three parts. The first part of an SSIS is the sensor(s), which monitors one or more process parameters over a specified range to detect the initiation of a safety significant event. The second part of an SSIS is the logic solver(s), which receives input from the sensor(s) and provides logic and/or math functions to generate a safety (SS) output signal to a final control element(s). The third part of an SSIS is the final control element(s) that performs the actual safety significant action. Figure 1 below provides a block diagram of an automatic SSIS. The listing of components shown in the figure for each part of an SSIS is given to provide examples and is not meant to be a complete listing.

Figure 1: SSIS Block Diagram – Automatic Actuation



- B. An operator can be included in an SSIS where operator actions are required to bring the facility or process system to a safe state. Figure 2 below provides a block diagram of an SSIS that includes operator action. The listing of components shown in the figure is given to provide examples and is not meant to be a complete listing.

Figure 2: SSIS Block Diagram – Operator Action



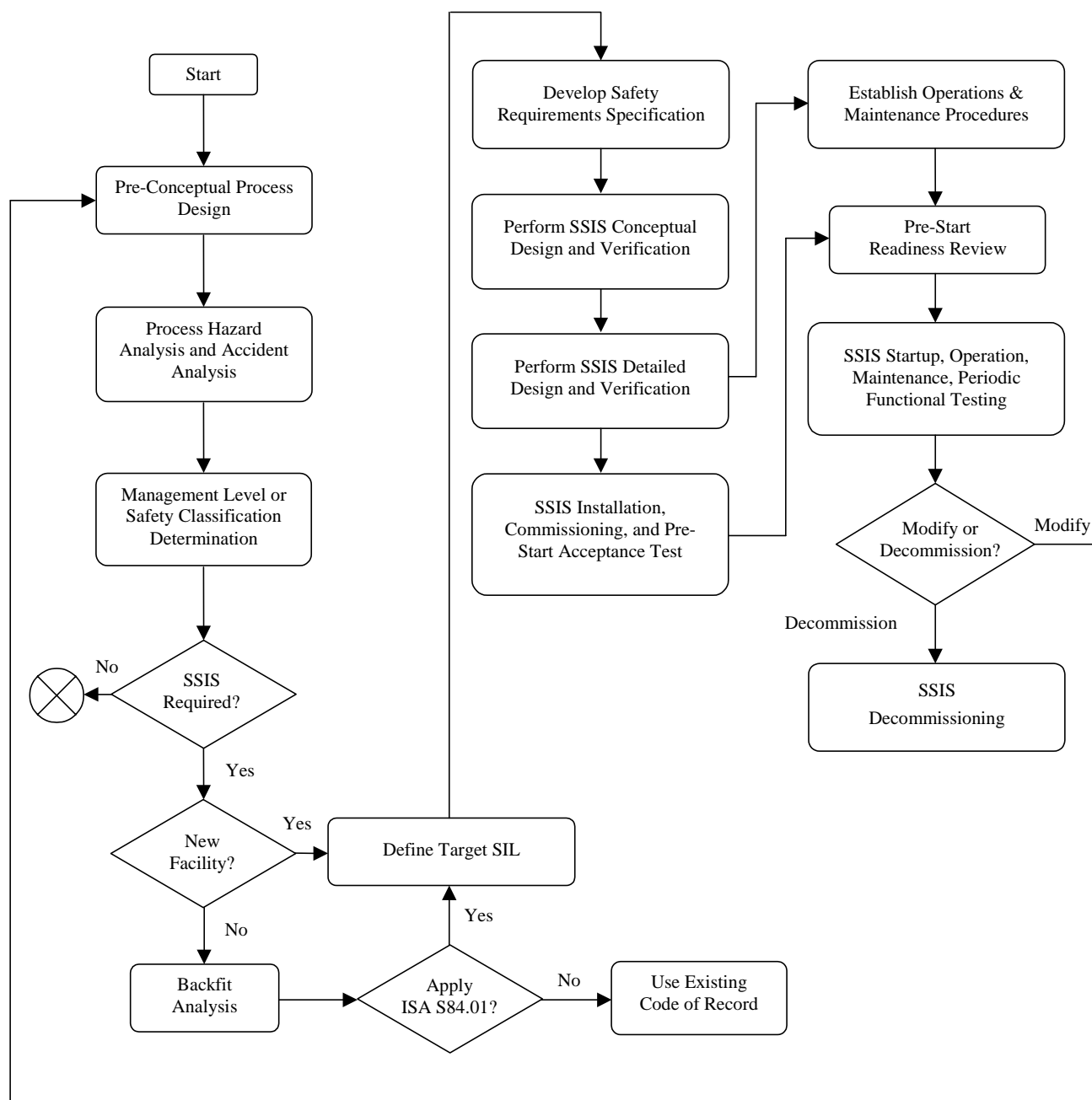
5.0 SYSTEM BOUNDARIES / CONSTRAINTS

- A. The SSIS includes all elements from the sensor to the final control element(s) that are required to perform the safety significant function, including inputs, outputs, support systems (e.g., electrical power, instrument air, ventilation, etc.), and logic solvers. Also included is hardware and software, including communication links, which are required to perform the safety significant function. Portions of the system that are not required to perform the safety significant functions and have no potential adverse impact on the performance of the safety significant functions are not considered part of the SSIS. These non-SS portions are not subject to the same design guidelines defined for the safety significant portions.

6.0 SSIS LIFE CYCLE

- A. ISA Standard 84.01 provides a Safety Life Cycle that covers the SSIS activities from initial conception through decommissioning. The following figure (Figure 3) depicts the SSIS life cycle approach.

Figure 3: SSIS Life Cycle Approach



7.0 DESIGN INPUTS

- A. The design requirement for the SSIS is established through the determination of a target Safety Integrity Level (SIL). The SIL defines the level of performance needed by the SSIS to reduce the likelihood or consequences of a hazardous event to an acceptable level. There are three SILs defined by ISA 84.01 (SIL-1, 2 & 3). The higher the SIL number the more likely the SSIS will be available to prevent or mitigate an SS event. The SIL performance requirements in terms of probability of failure on demand (PFD) average and risk reduction factor (RRF) are listed as follows:

SIL-1	PFD: 10^{-1} to 10^{-2}	RRF: 10 to 100
SIL-2	PFD: 10^{-2} to 10^{-3}	RRF: 100 to 1000
SIL-3	PFD: 10^{-3} to 10^{-4}	RRF: 1000 to 10,000

A methodology for determining the Safety Integrity Level for an SSIS is provided in Appendix A.

- B. Once the SIL level is established, the next step is to develop the Safety Requirements Specification for the SSIS design. Each SS function is generally unique and requires the identification of a specific set of performance requirements. The performance attributes should be identified and documented for each SS function and be provided by the Design Authority to the Design Agency. The following list of design input information should be considered along with information outlined in ANSI / ISA 84.01, Section 5, during the design of an SSIS or designated hazardous process protection layer:
1. Identification of the safety function. Define the state of the process. The complete description of the safety function should be provided including requirements such as the maximum allowed shutoff valve leakage. If the safe state involves sequencing, then the required sequencing should be identified.
 2. Required modes of operation.
 3. Target SIL of the SSIS.
 4. The required operating range and analytical safety limit of the system should be specified.
 5. The response time required of the system, including time for operator action, from the detection of a hazardous event to the completion of the final control element action should be specified.
 6. Environmental / Seismic design requirements.
 7. Desired system functional test interval.
 8. Maximum acceptable nuisance/spurious trip rate.
 9. Need for bypasses, manual trip or reset action by operator should be identified.
 10. Interfaces to other system. This would include 'status' inputs/outputs to/from other systems.

- C. The Design Authority should ensure that the Safety Requirements Specification for the SS function is available to the system designers at the start of the SSIS design. If a single technical agency is responsible for the total system implementation of the function, these inputs can be quantified for the overall function. However, if the design of the system is being performed through a number of technical agencies, the design input for the probability of failure on demand (PFD) and time response must be quantified for that portion of the design that each technical agency is responsible to complete. Examples for specifying these inputs amongst the different technical agencies are provided as follows:
1. Response Time Example:
The response time requirement for an SSIS has been identified as less than 30 seconds. The design of the sensors and logic solver has been assigned to one design agency and the design of the final control element (valve) has been assigned to a different technical agency. In meeting the required response time, the sensor and logic solver portion of the SSIS should be assigned a response time (e.g., less than 10 seconds) and the final control element should be assigned a response time (e.g., less than 15 seconds). This will allow the SSIS to meet its overall specification.
 2. PFD Example:
The PFD requirement for an SSIS has been identified as less than 10^{-2} (SIL-2). The PFD for the entire SSIS is the sum of the individual PFDs of the sensor, logic solver, and final control element. The design of the sensors and logic solver has been assigned to one design agency and the design of the final control element (valve) has been assigned to a different design agency. In meeting the required PFD, the sensor and logic solver portion of the SSIS should be assigned a PFD (e.g., less than 2×10^{-3}) and the final control element should be assigned a PFD (e.g., less than 5×10^{-3}). The summation of these two PFDs (7×10^{-3}) will satisfy the system level requirement of less than 10^{-2} . This will allow the SSIS to meet its overall specification.
- D. A checklist is provided in Appendix B that should be used as guidance in identifying design inputs, performing the design, and assessing the adequacy of the design. Not all items on the checklist are applicable for every SSIS and the checklist is not intended to cover all design considerations for all possible configurations. Furthermore, the checklist should not be a substitute for engineering judgement and good engineering practices, and strict adherence to the checklist does not necessarily guarantee a satisfactory design. However, judicious use of the list will increase the probability that a good design will be executed.

8.0 DESIGN CRITERIA

- A. Design criteria and guidelines will vary according to the specific system function and the required SIL level. ANSI / ISA 84.01, Annex B – SIS Design Considerations, provides guidance that should be considered in establishing the design criteria that is necessary to meet the SIL requirement of a particular SSIS.

- B. Systems should be designed so that the most probable failure modes of a system will increase the likelihood of a safe condition for the function. Additionally, systems should be designed as fail-safe. Attachment 2 of the I&C chapter provides guidance for the fail-safe design of process control loops. Note, however, that a system designed as fail-safe does not necessarily mean that any and all possible failures will result in the system going to a predetermined safe state.
- C. The safety significant functions of the system should not be interrupted or compromised by any non-safety significant functions performed by the system or by any other system.
- D. As indicated by ANSI / ISA 84.01, Section 7.4.1.3, safety signals should be hard wired and not multiplexed between the logic solver and field devices (sensor, final control element). Multiplexed signals (e.g., networks, data highways) can be used from a logic solver (e.g., PLC) to an alarm device if located in a manned area and operator action is required for the SSIS. Documentation of this configuration must demonstrate that the application meets the design criteria (PFD) for the function.
- E. Guidance on routing of safety significant wiring can be found in the I&C chapter, Section 11.2.
- F. The human-machine interface should be designed in accordance with the requirements defined by the Design Authority. The applicable criteria found in the I&C chapter, Section 10.0, and guidance provided in Attachment 5 should be considered in the design.
- G. An indication that the SSIS has performed the safety function should be provided to the operator. Indications that the SSIS has detected a full or partial system failure (trouble alarm) should also be provided to the operator.
- H. Systems that provide motive force (e.g., electrical power, instrument air) should be included as part of the SSIS evaluation only where they are required to complete the SS function.
- I. A certification should be provided for any safety PLC used in an SSIS. TUV and FM provide certification for components used in safety instrumented systems in the process industry. Note, however, that not all components certified to the same safety level (PFD) are equivalent. The certification reports will list restrictions on the operating conditions and the configuration of the components in order to achieve a specific PFD or SIL level. A certification report must be reviewed in its entirety to assure that components can be used in the selected design configuration to achieve the target SIL for the SSIS.
- J. As identified in Section 7.0, Item D, a checklist is provided in Appendix B that should be considered during the design process. An additional checklist for generic I&C systems is contained in Attachment 3 of the I&C chapter. This checklist should also be considered and used, as appropriate.

9.0 DESIGN VERIFICATION

- A. The required probability of failure on demand (PFD) is one of the key attributes that should be specified for safety significant functions through the SIL evaluation process. It is essential that the PFD of the SSIS be verified to assure that the SSIS as designed, installed, operated and maintained meets the target SIL specified for the system. The verification of the SSIS PFD should be conducted during the conceptual design in order to develop the SSIS design and at the end of the detailed design.
- B. The PFD of an SSIS should be verified by the application of Reliability Block Diagrams, Fault Tree Analysis, or Markov Models. Fault Tree Analysis is the preferred method for determining the PFD of the installed SSIS. Further guidance on the analysis of an SSIS can be obtained from draft ISA technical report TR84.00.02.
- C. An analysis team knowledgeable of the design being evaluated and ISA 84.01 should be convened to initiate the Fault Tree Analysis. The team typically consists of Design Agency, Design Authority, Safety Analysis engineers and a Fault Tree analyst. The team should agree on fault mechanisms, common mode failures, appropriate assumptions, etc., to be used to complete a preliminary Engineering Calculation based on the preliminary design of the SSIS. Other tools may be used to evaluate the PFD of the preliminary design. When the detailed design is complete, the team should reconvene to confirm the Calculation based on the final detailed design.
- D. Once an Engineering Calculation is completed for a final SSIS design, the calculation is maintained as a supporting document to the Authorization Basis for the facility.
- E. At the end of the detailed design phase the trip setpoint for the SSIS should be calculated. ANSI/ISA 67.04.01 should be used to establish the required trip setpoint of the safety function. The actual calibrated setpoint should provide sufficient allowance between the analytical limit and the calibrated instrument trip setpoint to account for uncertainties and dynamic responses.

10.0 BACKFIT ANALYSIS

- A. When an existing instrumented system is to be upgraded to Safety Significant / ML-2, the Design Authority refers to the Backfit Analysis for the system under consideration. This process establishes whether the instrumented system will meet the specific design, maintenance, and performance requirements of a Safety Significant System. If it is determined from the Backfit Analysis that a design modification is necessary to justify the upgrade of the system to an SSIS, the Design Authority initiates the ISA 84.01 process.

Appendix A: Safety Integrity Level Assignment Methodology

This methodology defines the necessary steps for assigning a target Safety Integrity Level (SIL) to Safety Significant Instrumented Systems. The methodology is based on a frequency and consequence ranking matrix recognized by DOE-STD-3009 and further developed through the LANL Hazard Analysis Technical Methodology Manual. The calculation of the target SIL is based on the credit taken for the SSIS to reduce the likelihood or consequence of the hazardous event to an acceptable level.

Laboratory Implementation Guidance LIG 230-01-02.0, Graded Approach for Facility Work, defines key factors within the ML-2 listing for Safety and Health that identify SS functions required to satisfy public safety, worker safety, and defense in depth at LANL. Key factors that identify SS functions required to protect the environment are provided within the ML-2 listing for Environmental Consequences. The SS functions are satisfied through control features, which can either be engineered systems, administrative controls, or passive controls. Safety Significant Instrumented Systems (SSISs) are a subset of design features that may be designated to provide an SS function to prevent or mitigate a hazardous condition or event. This methodology is only concerned with assigning SIL levels for SSISs.

The SIL level of an SSIS cannot be determined without looking at all of the SS SSCs and administrative controls that may be credited with providing the safety function to prevent or mitigate a specific hazardous event. This methodology assesses the required risk reduction for the SS hazardous event. In some cases, the SSIS alone is required to provide the entire risk reduction for the hazardous event. In other cases, the SSIS in combination with other credited design features and controls provides the required risk reduction. The quality of the SSIS design that is required to reduce the overall risk of the hazardous event to an acceptable level is based on the risk reduction provided by all of the credited design features and controls.

As established within LIG 230-01-02.0, Graded Approach for Facility Work, SS functions are identified through the following Key Factors:

- | | |
|----------|--|
| Factor 1 | SSC is designated as Safety Significant per DOE-STD-3009-94. |
| Factor 2 | SSC failure could cause the failure of another Safety Significant SSC or prevent it from performing its required function. |
| Factor 3 | SSC is required to support another Safety Significant SSC. |
| Factor 4 | SSC failure could cause or allow release of radioactive material with a potential radiological dose less than 25 rem or releases of chemicals with a potential does less than ERPG-2 per DOE-STD-3009-94 at the site boundary. |
| Factor 5 | SSC provides defense in depth, backup, or redundancy to a Safety Class SSC. |
| Factor 6 | SSC failure could result in death or serious (disabling) injury or illness to a worker. |
| Factor 7 | SSC failure could result in minor injury, irritation, annoyance, or illness to a member of the public. |
| Factor 8 | SSC failure could cause or allow severe long-term damage to the environment within Laboratory boundaries. |
| Factor 9 | SSC failure could cause or allow damage to commercial resources such as agricultural, recreational, or business properties. |

SIL Assignment for SS Key Factors 1, 4, 6, 7, 8 & 9

For Factors 1, 4, 6, 7, 8 and 9 functions are classified SS based on the results of a Hazard Analysis (HA). The HA identifies abnormal occurrences and potential accident scenarios that could cause harm to the public, worker, or environment and determines the unmitigated consequences and expected frequency of each particular event. The unmitigated consequences are generally established through a quantitative analysis for nuclear and chemical hazards and through qualitative analysis for other hazards (e.g., high explosives). The unmitigated event frequency is generally established through a qualitative process that is based primarily on engineering judgement.

Once the unmitigated consequences and frequency have been established, the events are assigned to a “bin” of a frequency-consequence risk matrix to assess the relative risk. The method of risk binning allows for attention to be focused on those events that pose the greatest risk to the public, workers, and the environment. The figures on the following pages are representations of the frequency-consequence risk matrices developed by LANL for the public and the worker as identified within the LANL Hazard Analysis Technical Methodology Manual.

Figure A1: Public Hazard Risk Matrix



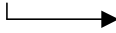

Likelihood  Consequence 	Frequent (Expected) $> 10^0/\text{yr.}$	Probable (Likely) $< 10^0/\text{yr. to}$ $> 10^{-2}/\text{yr.}$	Occasional (Unlikely) $< 10^{-2}/\text{yr. to}$ $> 10^{-4}/\text{yr.}$	Improbable (Extremely Unlikely) $< 10^{-4}/\text{yr. to}$ $> 10^{-6}/\text{yr.}$	Remote (Beyond Extremely Unlikely) $< 10^{-6}/\text{yr.}$
High $> 25 \text{ Rem TEDE}$ $> \text{ERPG-2}$	1	1	2	2	3
Medium From $> 5 \text{ Rem}$ to $< 25 \text{ Rem}$ From $> \text{ERPG-1}$ to $< \text{ERPG-2}$	1	2	2	3	3
Low From $> 0.1 \text{ Rem}$ to $< 5 \text{ Rem}$ From Measurable to $< \text{ERPG-1}$	1	2	3	3	4
Negligible $< 0.1 \text{ Rem}$ $< \text{Measurable}$	3	3	3	4	4
None	4	4	4	4	4













Figure A2: Worker Hazard Risk Matrix

Likelihood  Consequence 	Frequent (Expected) $> 10^0/\text{yr.}$	Probable (Likely) $< 10^0/\text{yr. to}$ $> 10^{-2}/\text{yr.}$	Occasional (Unlikely) $< 10^{-2}/\text{yr. to}$ $> 10^{-4}/\text{yr.}$	Improbable (Extremely Unlikely) $< 10^{-4}/\text{yr. to}$ $> 10^{-6}/\text{yr.}$	Remote (Beyond Extremely Unlikely) $< 10^{-6}/\text{yr.}$
High Immediate Health Effects or Loss of Life	1	1	2	2	3
Medium Long-term Health Effects, Disability, or Severe Injury (non life threatening)	1	1	2	3	4
Low Lost-time Injury but No Disability (work restriction)	1	2	3	4	4
Negligible Minor Injury with No Disability and No Work Restriction	2	3	4	4	4
None	4	4	4	4	4

Identifying Risk Reduction Goals

The hazard analysis provides the assigned risk-bin for a postulated accident scenario that require SS controls and identifies all of the control features that are credited with preventing or mitigating the SS hazardous event. The objective of SSCs and Administrative Controls (ACs) identified as SS control features are to reduce the consequences and/or frequency of the event in order to reduce the relative risk. The design of an SSIS is considered to provide adequate prevention or mitigation for an event if the risk reduction provided by the SSIS alone or the SSIS in combination with other SS features reduces the risk by an acceptable margin. The risk reduction provided by an SSIS designed to one of the three SILs is graphically illustrated on the following Risk Binning Matrix.

Figure A3: SIL Reduction Risk Binning Matrix

Likelihood  Consequence 	Probable (Likely) $< 10^0/\text{yr. to}$ $> 10^{-2}/\text{yr.}$	Occasional (Unlikely) $< 10^{-2}/\text{yr. to}$ $> 10^{-4}/\text{yr.}$	Improbable (Extremely Unlikely) $< 10^{-4}/\text{yr. to}$ $> 10^{-6}/\text{yr.}$	Remote (Beyond Extremely Unlikely) $< 10^{-6}/\text{yr.}$
High $> 25 \text{ Rem TEDE}$ $> \text{ERPG-2}$			   	
Medium From $> 5 \text{ Rem}$ to $< 25 \text{ Rem}$ From $> \text{ERPG-1}$ to $< \text{ERPG-2}$		  		
Low From $> 0.1 \text{ Rem}$ to $< 5 \text{ Rem}$ From Measurable to $< \text{ERPG-1}$				
Negligible $< 0.1 \text{ Rem}$ $< \text{Measurable}$		Note: The arrows represent the range of risk reduction provided by the different SIL levels. The solid portion of the arrows represent the minimum risk reduction provided by the designated SIL. The dotted portion of the arrows represent the minimum and maximum range of risk reduction that can be achieved by the SIL.		

Determination of a Target SIL for an SSIS using a Layer of Protection Analysis (LOPA)

Each of the protective features identified within the hazard analysis as a primary (1st Level of Control) is considered a layer of protection. The hazard analysis process should quantify the expected effectiveness of the layers of protection that are not SSISs in terms of Probability of Failure on Demand (PFD) or availability. If the hazard analysis does not quantify the required PFD or availability of a credited SS system or control, then this must be determined separately before the SSIS SIL can be assigned. Where a system already exists and has been designated as a preventive or mitigation feature, verification of its safety availability is required to determine its effective PFD.

A Layer of Protection Analysis (LOPA) is used to determine the required SIL of the SSIS. A LOPA is a form of risk assessment, similar to that of an event tree analysis, in which two outcomes are considered, failure (PFD) or successful operation. The frequency of the unmitigated hazardous event in question is the starting point of the LOPA. If the hazard analysis process identifies a specific event frequency for a hazard, then this value should be used in the LOPA calculation. However, where a qualitative analysis provides the unmitigated event frequency in terms of Probable, Occasional, or Improbable, the midpoint of the frequency range for the respective bin should be used as listed below, providing that the analysis is conservative.

Probable (Likely)	$10^{-1}/\text{yr}$
Occasional (Unlikely)	$10^{-3}/\text{yr}$
Improbable (Extremely Unlikely)	$10^{-5}/\text{yr}$

A Basic Process Control System (BPCS) may be used, in combination with the assigned unmitigated event frequency, to calculate a mitigated event frequency for an SS hazardous event. However, the following conditions must be met to allow the inclusion of the BPCS in the event frequency calculation:

1. The failure of the BPCS is not the initiating or contributing cause of the event.
2. The BPCS must be designed to function during the event, including the environmental conditions for which it is credited for operation.
3. A risk reduction factor claimed for the BPCS must be ten or less ($\text{PFD} \geq 10^{-1}$).
4. SSCs that monitor initial conditions and are credited in a LOPA analysis for reducing or establishing the initial event frequency cannot be a part of a BPCS that is also credited in the LOPA analysis. BPCS must be independent of the event initiator or other Layers of Protection.

Once the event frequency has been established, the LOPA process consists of the identification of each Independent Protection Layer (IPL) and an evaluation into the effectiveness that each has in preventing and/or mitigating the SS or designated ML-2 hazardous event. Independent Protection Layers (IPLs) may include but are not limited to: (1) design features such as siting, containment, confinement, and shielding, (2) administrative controls that restrict deviations from safe operations through operating procedures or limiting conditions of operation, (3) mechanical or process systems, and (4) an SSIS. Note: Administrative controls require consideration of the human interface in sensing conditions and performing functions.

General rules for IPLs:

1. The IPL must be designed to prevent an SS hazardous event, or mitigate the consequences of such an event to an acceptable level.

2. A system, structure, component that is classified as safety class or safety significant, TSR administrative control, or other SSC that is adequately identified and controlled in the requirements of the Authorization Basis of a facility can be considered as an IPL.
3. The IPL is designed to perform a safety function during normal, abnormal and design basis accident environmental conditions for which it is required to operate.
4. IPLs must be sufficiently independent so that the failure of one IPL does not adversely affect the probability of failure of another IPL.

If some combination of components or systems is required to function together to protect a worker or the public, they should be considered as one IPL. Thus, if it takes two out of three components to function or a series of components to operate to protect a worker, then the combination of SSCs will constitute one IPL. The IPL may not by itself reduce the risk of the hazardous event occurring to an acceptable level, but it will prevent or mitigate the event to an acceptable level when it works.

Given that the IPL design follows the above rules, then the SS hazardous event and the IPL failure can be treated as statistically independent occurrences. Thus, both the hazardous event and a failure of all IPLs must occur before there is an unacceptable result. If any of the IPLs function, then the event will be prevented or mitigated to an acceptable level.

LOPA is based on calculating the probability of a series of independent events occurring. The event must occur and all IPLs must fail in order for the hazardous event to affect the workers or public. As an example probability calculation, the probability of failure (likelihood) of getting three IPLs (A, B, and C) to fail is shown below (three input AND gate):

$$P(A \cap B \cap C) = P(A) \times P(B) \times P(C)$$

\cap \equiv Symbol for AND

P(Z) is the PFD of IPL (Z)

The goal of an IPL is to prevent a hazardous event from occurring or mitigate the hazardous event to an acceptable level. Whether the IPL is designed to prevent or mitigate the event, the PFD of the IPL is used in the LOPA calculation. The probability of the undesired consequence is based on the product of the unmitigated event frequency and all of the PFDs of the separate independent protection layers.

The SSIS SIL calculated from the LOPA analysis should provide the capability of a one-half decade risk reduction beyond the minimum risk reduction required to reduce the likelihood of the event by an acceptable margin. The one-half decade risk reduction, beyond that minimally required to place the event into an acceptable risk bin, provides a degree of assurance against uncertainties in event frequencies, component failure rates, and other terms used in the calculation to verify the target SSIS SIL.

Sample SIL Determinations

Included below are examples of the use of a LOPA to assign SSIS SIL levels. The order of the IPLs in a LOPA diagram is unimportant to the calculation of the required SIL level.

As can be seen in the example calculations, Administrative Controls are one of the layers of protection that can be taken credit for in a LOPA analysis. Administrative Controls are assigned for the programs and administrative requirements that ensure that the basic facility conditions assumed in the analysis do exist (e.g., minimum staffing limits and established inventory control programs). Administrative Controls are also assigned to procedural or program controls or equipment that perform a passive function that the operator does not directly control (e.g., inventory control based on records of installed measurement equipment or passive barriers credited in the accident analysis).

Example 1

The following is a target SIL determination for a hazardous event that is anticipated with high consequences. The design uses three Independent Protection Layers (IPLs) to reduce the likelihood of the event to less than 10^{-6} /yr.

Unmitigated Hazardous Event	IPL-1 (SSC)	IPL-2 (SSIS)	IPL-3 (AC)	Unacceptable Consequence Likelihood
Event (High Consequences)	SSC Fails PFD= 10^{-2}	SSIS Fails PFD=???	AC Fails PFD= 10^{-1}	Likelihood Goal < 10^{-6} /yr. { 10^{-6} to 10^{-7} }
Frequency (10^{-1} /yr.)	<div>AC Operates</div> <div>SSIS Operates</div> <div>SSC Operates</div>			No Impact

Calculation:

$$\begin{aligned}
 \text{Frequency} \times \text{PFD}_{\text{IPL-1}} \times \text{PFD}_{\text{IPL-2}} \times \text{PFD}_{\text{IPL-3}} &< 10^{-6}/\text{yr.} \\
 (10^{-1}/\text{yr.}) \times (10^{-2}) \times \text{PFD}_{\text{IPL-2}} \times 10^{-1} &< 10^{-6}/\text{yr.} \\
 \text{PFD}_{\text{IPL-2}} \times 10^{-4}/\text{yr.} &< 10^{-6}/\text{yr.} \\
 \text{PFD}_{\text{IPL-2}} &< 10^{-2}/\text{yr.}
 \end{aligned}$$

Thus, the SSIS (IPL-2) should be designed as a SIL-2 (PFD: 10^{-2} to 10^{-3}). A SIL-2 SSIS, in combination with the other IPLs, has the capability to reduce the likelihood of the unacceptable consequences for this event to 10^{-7} /yr.

Example 2

The following is a target SIL determination for a hazardous event that is unlikely with medium consequences. The design uses only one Independent Protection Layer (IPL) to reduce the likelihood of the event to less than 10^{-4} /yr.

Unmitigated Hazardous Event	IPL-1 (SSIS Alarm System / Operator Action)	Unacceptable Consequence Likelihood
Event (Medium Consequence)	SSIS Alarm System Fails	Likelihood
	PFD=???	Goal $< 10^{-4}$ /yr. { 10^{-4} to 10^{-5} }
	SSIS Alarm System Operates	No Impact
Frequency (10^{-3} /yr.)		

Calculation:

$$\begin{aligned}
 \text{Frequency} \times \text{PFD}_{\text{IPL-1}} &< 10^{-6}/\text{yr.} \\
 (10^{-3}/\text{yr.}) \times \text{PFD}_{\text{IPL-1}} &< 10^{-6}/\text{yr.} \\
 \text{PFD}_{\text{IPL-1}} &< 10^{-1}/\text{yr.}
 \end{aligned}$$

Thus, the SSIS (IPL-1) should be designed as a SIL-1 (PFD: 10^{-1} to 10^{-2}). A SIL-1 SSIS has the capability to reduce the likelihood of the unacceptable consequences for this event to 10^{-5} /yr.

Example 3

The following is a target SIL determination for a hazardous event that is unlikely with high consequences. The design uses three Independent Protection Layers (IPLs) to reduce the likelihood of the event to less than 10^{-6} /yr.

Unmitigated Hazardous Event	IPL-1 (SSC)	IPL-2 (SSIS)	IPL-3 (AC)	Unacceptable Consequence Likelihood
Event (High Consequences)	SSC Fails PFD= 10^{-2}	SSIS Fails PFD=???	AC Fails PFD= 5×10^{-2}	Likelihood Goal < 10^{-6} /yr. { 10^{-6} to 10^{-7} }
Frequency (10^{-3} /yr.)	<div>AC Operates</div> <div>SSIS Operates</div> <div>SSC Operates</div>			No Impact

Calculation:

$$\begin{aligned}
 \text{Frequency} \times \text{PFD}_{\text{IPL-1}} \times \text{PFD}_{\text{IPL-2}} \times \text{PFD}_{\text{IPL-3}} &< 10^{-6}/\text{yr.} \\
 (10^{-3}/\text{yr.}) \times (10^{-2}) \times \text{PFD}_{\text{IPL-2}} \times (5 \times 10^{-2}) &< 10^{-6}/\text{yr.} \\
 \text{PFD}_{\text{IPL-2}} \times (5 \times 10^{-7}/\text{yr.}) &< 10^{-6}/\text{yr.} \\
 5 \times 10^{-7}/\text{yr.} &< 10^{-6}/\text{yr.}
 \end{aligned}$$

The SSIS providing the IPL-2 in this example is not required because IPL-1 and IPL-3 provide a combined risk reduction factor in conjunction with the event frequency that achieves the goal of reducing the likelihood of the event. If IPL-1 (SSC) were an instrumented system it would be designated as an SSIS.

Example 4

The following is a target SIL determination for a hazardous event that is anticipated with high consequences. The design takes credit for the operation of the Basic Process Control System (BPCS), which if operating would prevent the event condition from occurring, in addition to two Independent Protection Layers (IPLs) to reduce the likelihood of the event to less than $10^{-6}/\text{yr.}$

Unmitigated Hazardous Event	BPCS Event Mitigation	IPL-1 (SSC)	IPL-2 (SSIS)	Unacceptable Consequence Likelihood
Event (High Consequences)	BPCS Fails	SSC Fails	SSIS Fails	Likelihood
		PFD= 10^{-2}	PFD=???	Goal < $10^{-6}/\text{yr.}$ { 10^{-6} to 10^{-7} }
		SSC Operates	SSIS Operates	No Impact
Frequency ($10^{-1}/\text{yr.}$)	PFD= 10^{-1}			

Calculation:

$$\begin{aligned}
 \text{Frequency} \times \text{PFD}_{\text{BPCS}} \times \text{PFD}_{\text{IPL-1}} \times \text{PFD}_{\text{IPL-2}} &< 10^{-6}/\text{yr.} \\
 (10^{-1}/\text{yr.}) \times (10^{-1}) \times (10^{-2}) \times \text{PFD}_{\text{IPL-2}} &< 10^{-6}/\text{yr.} \\
 \text{PFD}_{\text{IPL-2}} \times (10^{-4}/\text{yr.}) &< 10^{-6}/\text{yr.} \\
 \text{PFD}_{\text{IPL-2}} &< 10^{-2}/\text{yr.}
 \end{aligned}$$

Thus, the SSIS (IPL-2) should be designed as a SIL-2 (PFD: 10^{-2} to 10^{-3}). A SIL-2 SSIS, in combination with IPL-1, has the capability to reduce the likelihood of the unacceptable consequences for this event to $10^{-7}/\text{yr.}$

SIL Assignment for SS Key Factors 2 & 3

A SIL is not assigned to an SS system that provides a supporting function to or enables the performance of another ML-1, SC, ML-2, or SS safety system. However, support systems (e.g., electrical power, instrument air, cooling water, ventilation) do have a strong influence on SSIS performance. Ultimately, the support systems may determine whether or not the SSIS meets its target SIL. Nonetheless, SILs are assigned only to SSISs, not to support systems.

Although support systems to ML-2 or SS systems are not assigned a SIL, the PFD of the support system is generally required to determine the PFD of the overall SSIS system. The support system availability may have a significant impact on whether or not the SSIS will achieve its targeted SIL.

The PFD of a support system is also used in calculations to determine the PFD of non-SSIS systems for which it supports, where the non-SSIS functions may be credited in a LOPA analysis.

SIL Assignment for SS Key Factor 5

The Hazards Analysis process results in a minimum number of LOCs that are necessary for the protection of workers and the public. Additional LOCs (2nd and 3rd Levels of Control) may also be selected so that no one layer of protection is completely relied on to prevent or mitigate a hazardous event. An SSIS may be selected as an additional LOC if the system functions as defense in depth, backup, or redundant to a function designated as SC.

The LANL Hazards Analysis Technical Methodology Handbook provides criteria to aide in the selection of LOCs. This criteria specifies that preventive controls should be selected over mitigation controls. A preventive first level LOC is generally required to reduce the frequency of the event in order to reduce the relative risk. Where an SSIS LOC is providing a second or third LOC for a preventive system, then the SSIS should be designed to meet SIL-1 requirements as a minimum. A SIL-1 SSIS is an independent safety protection layer that can be readily expected to mitigate or prevent an unwanted event.

If the SSIS is providing a second LOC for an existing primary (1st LOC) ‘mitigation’ system, additional consideration should be provided in determining the required SIL. An SSIS that provides the second LOC for a mitigation system should be designed to meet SIL-1 requirements as a minimum, and if possible should prevent the hazardous event. For a ‘Probable’ event, where a preventative SSIS can be selected as an additional LOC for a mitigation primary LOC, a SIL-2 or SIL-3 SSIS should be considered.

Appendix B: Safety Significant Instrumented System Checklist

Design Input

Safety Significant (SS) Design Input

1. Has the Hazard Analysis identified the consequence and event frequency for each SS function?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Has the Safety Integrity Level been assigned for each SS function?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Has a time response been assigned for each SS function?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4. Has a setpoint and range been assigned for each SSIS process parameter?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Conceptual Design

1. Has the Safety Integrity Level been verified for each SS function?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Did an independent assessor review the conceptual design? Note: An independent assessor is considered to be any qualified individual competent enough to have prepared the design but sufficiently independent such that they are not verifying their own design.	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Detailed Design

Operator Interface

1. Are controls and displays adequate, effective, and suitable for operator tasks?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Is the SSIS operation consistent with existing systems, established conventions and operator experience?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Do separate displays present consistent information?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4. Does the indication at the operator display show information that is consistent with the related control action or process response to a control or safety action?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5. Is displayed information readable, concise, complete, and usable without extrapolation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6. Is adequate information about normal and upset conditions displayed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
7. Is display failure readily apparent?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
8. Are instruments located at recommended height and reach limits?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
9. Are critical alarms obvious to an operator?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
10. Are related controls, displays, and alarms grouped together?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
11. Is manual initiation of the SSIS provided?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

12. Is the possibility of accidental operator activation of SSIS initiation minimized?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
13. Does the SSIS require a manual reset to clear the SSIS interlock and resume operations?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
14. Is the SSIS in an area that requires frequent operator attention?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
15. Do displays support operator task requirements in terms of range, precision and accuracy?			
16. Are normal operating ranges and alarm setpoints clearly identified?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Sensors

1. Is sensor redundancy employed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. If identical redundancy is employed, has the potential for common cause failure been adequately addressed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Are redundant sensors installed with adequate physical separation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4. Does each sensor have dedicated wiring to the SSIS I/O modules?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5. Does each sensor have a dedicated process tap?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6. Does the configuration allow each sensor to be independently proof tested?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
7. Can redundant sensors be tested or maintained without reducing the integrity of the SSIS?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
8. Is diversity used?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
8.1 Are diverse parameters measured?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
8.2 Are diverse means of processing specified?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
9. Is there sufficient independence of hardware manufacturer?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
10. Is there sufficient independence of hardware test methods?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
11. Are sensor/instrument sensing lines adequately purged or heat traced to prevent plugging?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
12. Are SSIS sensors clearly identified by some means (tagging, paint, etc) as components of the SSIS?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
13. Has the mean time to dangerous failure rate been determined for each sensor?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Logic Solver

1. Does the logic solver have methods to protect against fail-dangerous faults?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Is the logic solver a fault-tolerant device?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Is the logic solver separated from the Basic Process Control System?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4. Are all SS functions combined in a single logic solver?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5. Is the logic solver TUV or FM certified for the application?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6. Is the application software protected from unauthorized changes?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
7. Has the mean time to dangerous failure been determined for the logic solver?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Application Software

1. Is the final program verified through factory acceptance testing that includes fault simulation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Is the final program verified through complete site acceptance testing that includes verification of startup, operation, and testing algorithms?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Has software met design criteria?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Actuators

1. Are backup power sources provided?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Are manual actuators safely and easily accessible?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Final Elements

1. Have the final elements been checked to ensure proper sizing and application?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Have the final elements been checked to ensure that the devices achieve the fail-safe condition?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Has the mean time to dangerous failure rate been determined for each final element?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Process Connections

1. Are process connections properly installed to prevent process fouling?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Are process connections installed correctly for the device type and process?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Are sensor process isolation valves associated with the SSIS properly marked?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Electrical Connections/Conduit/Wire-Trays/Junction Boxes

1. Are electrical connections properly made and inspected?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Are all SSIS conduits/wire-trays properly marked?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Are all SSIS conduits/wire-trays adequately segregated from non-SSIS conduits/wire-trays?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4. Are all conduit covers and gaskets in place?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5. Are all seals poured?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6. Are all SSIS junction boxes properly marked?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
7. Are all SSIS terminations in shared junction boxes adequately segregated from non-SSIS terminations?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
8. Is the electrical power source reliable?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
9. Have the consequences of loss of instrument power been considered?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
10. Is there an Uninterruptible Power Supply (UPS) for the SSIS?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
10.1 Is it periodically tested?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
11. Are primary and backup supplies powered from independent busses?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
12. Can redundant supplies be taken out of service for maintenance without interrupting SSIS operation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
13. Is the SSIS properly grounded?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
14. Is the SSIS hardware consistent with the area electrical classification?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
15. Are the power supplies adequately protected from ground faults or other voltage disturbances?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Pneumatic Supply

1. Is the pneumatic supply source clean and reliable?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Have the consequences of loss of pneumatic supply been considered?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Have the consequences of over-pressure of the pneumatic supply been considered?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Hydraulic Supply

1. Is the hydraulic supply source clean and reliable?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Have the consequences of loss of hydraulic power been considered?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Have the consequences of over-pressure of the hydraulic power been considered?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Environmental

1. Have the effects of RFI on the SSIS devices been considered?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Are the devices being used within the manufacturer's environmental specifications?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Have sources of excessive vibration been eliminated or mitigated?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4. Have sources of excessive temperature been eliminated or mitigated?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5. Have all SSIS seismic requirements been achieved?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6. Have the effects of the total integrated radiation dose on components been considered?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
7. Have all SSIS component environmental requirements been achieved?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Installation / Operation
Installation

1. Have external causes of common cause failure been identified (e.g., fire, vehicle impact, lightning, etc.)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Is the SSIS segregated from other systems to minimize the probability of external influences causing a simultaneous failure of the systems?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Is there sufficient separation in the installation of diverse equipment?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Operation

1. Are operators provided separate, specific SS procedures?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Are operators provided specific training relative to the SS system?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Are operators being evaluated for competency in SS operation on a regular basis?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Testing / Maintenance
Testing

1. Does the periodic test interval for the SSIS and components meet the SIL verification assumptions?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. If a component fails under test, is the failure cause established to identify manufacturing or design defects?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. If a redundant element fails, do procedures require the inspection of other elements for similar faults?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4. Is there adequate independence of testing methods for diverse systems?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Maintenance

1. Are maintenance bypasses alarmed to the control room?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Are operators trained on what to monitor when maintenance bypasses are used?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

ENDNOTES:

ATTACHMENT 2

FAIL-SAFE DESIGN OF PROCESS CONTROL LOOPS (PROGRAMMATIC AND FACILITY)

TABLE OF CONTENTS

1.0	PURPOSE	2
2.0	SCOPE	2
3.0	DEFINITIONS	2
4.0	FAIL-SAFE ANALYSIS	2
5.0	FAIL-SAFE DESIGN PRINCIPLES	3
6.0	FAIL-SAFE TRANSMITTER CONFIGURATION	4
7.0	FAIL-SAFE CONTROLLER CONFIGURATION.....	7
8.0	FAIL-SAFE CONTROL ELEMENT CONFIGURATION	8

RECORD OF REVISIONS

Rev	Date	Description	POC	OIC
0	10/--/03	Initial issue	Mel Burnett, <i>FWO-DECS</i>	Gurinder Grewal, <i>FWO-DECS</i>

1.0 PURPOSE

This attachment provides guidance for designing fail-safe process control loops.

2.0 SCOPE

Fail-safe protection is considered for loss of electrical power or air supply to any element in the instrument loop and for loss of the control signal to any valve or instrument in the control loop or between interconnected loops. The effects of sensing element failures are also discussed, as well as the affect of digital controller configuration details on loop reliability and safety. Items not considered are internal failures in instruments and retaining the last valve positioned after a failure.

3.0 DEFINITIONS

Direct Action – A device in which the value of the output signal increases as the value of the input (measured variable or controlled variable) increases.

Fail-Safe – A design characteristic by which a unit or system will attain a safe state and remain safe if a system or component loses its activation energy.

Intrinsically Safe – Equipment and wiring that are incapable of releasing sufficient electrical or thermal energy under normal or abnormal conditions to cause ignition of a specific hazardous atmospheric mixture in its most easily ignited concentration.

Overrange – Any excess value of an input signal above its upper range value or below its lower range value. The overrange limit is the maximum input that can be applied to a device without causing damage or permanent change in performance.

Reverse Action – A device in which the value of the output signal decreases as the value of the input (measured variable or controlled variable) increases.

Sensor – A device that responds to a physical stimulus from a process variable and converts the measurement into an electric or pneumatic signal.

Transmitter – A device that responds to the value of a measured variable and transmits a resulting signal. A transmitter may contain a sensor to directly monitor a process variable.

4.0 FAIL-SAFE ANALYSIS

- A. The fail-safe analysis should establish the potential faults of each individual component within the process control loop and evaluate their effects on the final control element and the process.
- B. The fail-safe analysis should determine the “safe direction” of the process medium that is measured to establish the desired response of the process control loop for potential faults and component failures. The Hazards Analysis, or other safety analyses, should be consulted for this information and reviewed as part of the fail-safe analysis. As an example, the safe direction when measuring temperature or pressure is usually toward lower temperature or pressure. However, for other measured mediums, the opposite direction may be safest.

- C. The fail-safe analysis should identify the motive force(s) required for the operation of each component within the process control loop (e.g., power supplies, instrument air, hydraulics, etc.). In analyzing the ability of a process control loop to fail in the safest direction, the potential failure of the motive force(s) should be evaluated not only for their effect on the individual components but also for their effect on the final output response of the process control loop.
- D. The fail-safe analysis should evaluate the effects of a loss or failure of the control signal on the individual components and the resulting effect on the final output response of the process control loop. The control signal is considered to be any command, actuation, alarm, or data signal(s) that is required to start, stop, or continue some operation.

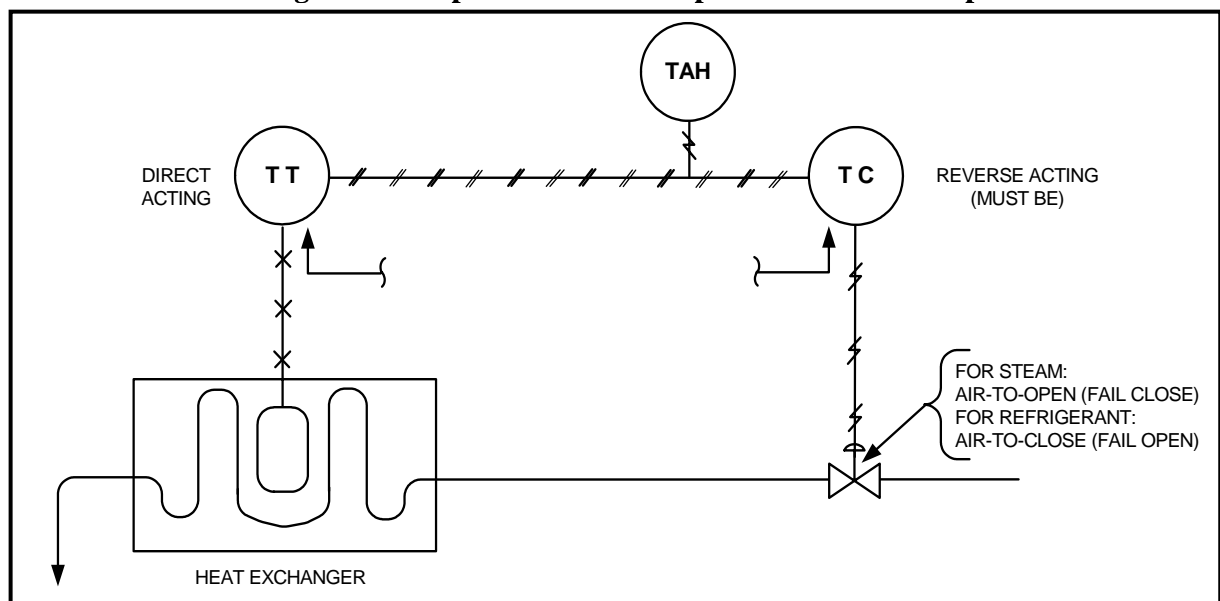
5.0 FAIL-SAFE DESIGN PRINCIPLES

- A. Fail-safe design can generally be implemented through the use of either direct action or reverse action sensors. A reverse action sensor should be used when a high value of process variable is unsafe and a direct action sensor should be used when a low value of process variable is unsafe. The fail-safe analysis should make the determination which type sensor is required and ensure that it results in a fail-safe condition. In some instances it may appear that the use of either a direct action or reverse action will result in a fail-safe process control loop, but this is not always the case. For example, a thermistor has a negative temperature coefficient of resistance and would seem to qualify as a reverse action sensor. However, since short circuits and open circuits would produce opposite results at the receiver, it is not fail-safe. Only when the sensor produces its own outputs can both short circuits and open circuits result in output signal loss (e.g., thermocouples).
- B. Where a reverse action sensor is preferred but not available, signal reversal should take place as soon as possible in the process control loop. For example, an application involving a thermocouple-to-pneumatic converter in which reverse action is necessary, the reversing action should take place in the signal amplifier rather than in the current-to-pressure (I/P) transducer. In most applications, however, a reverse action transmitter will ensure that signal reversal occurs at the nearest possible point within the process control loop.
- C. In addition to the implementation of direct action or reverse action sensors / transmitters, the design of a fail-safe process control loop should take into consideration the following design principles.
 - 1. Design Integrity and Quality
 - 2. Redundancy or Backup Systems
 - 3. Isolation of Systems, Components, and Elements
 - 4. Reliability
 - 5. Failure Warning or Indication
 - 6. Maintainability

6.0 FAIL-SAFE TRANSMITTER CONFIGURATION

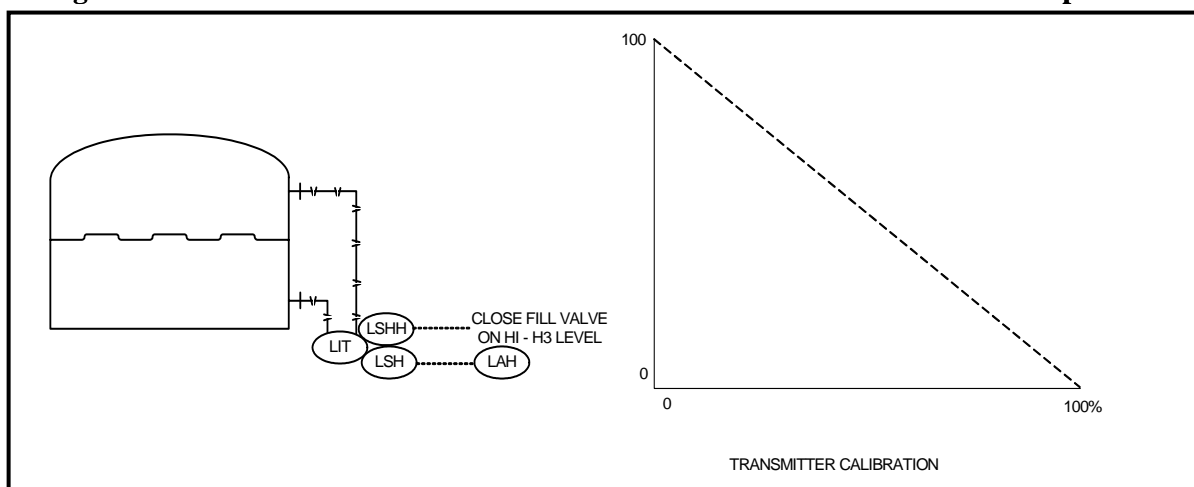
- A. The loss of a transmitter output signal should cause a fail-safe action. A transmitter is considered to be any device that responds to the value of a measured variable and transmits a resulting signal. The transmitter may contain the sensor.
- B. Short circuits, open circuits, and grounds may all cause the loss of a transmitter output signal. For a four-wire transmitter, the transmitter power is brought in on one pair of wires and the output signal is brought out on another pair. All 3 types of electrical failures in either the power or signal wiring pair result in loss of signal to the receiver. Partial shorts will lower the signal for either a current or voltage output signal. Under certain circumstances, full or partial shorts between particular power and signal wires could cause erroneous high signal indications. However, the likelihood of this latter occurrence is small.
- C. For a three-wire transmitter, the output and power circuits share a single common conductor, but otherwise the considerations are the same as for the four-wire transmitter.
- D. The unsafe action of an instrument loop due to the loss of the transmitter output signal can be illustrated by using a pneumatic temperature control loop as an example, see Figure 1 below. Assume that high temperature is unsafe and a direct action transmitter is used in the loop. A high pneumatic signal will therefore represent a high temperature. Accordingly, the controller interprets a full or partial loss of signal as a low temperature and attempts to correct the condition. The high-temperature alarm would not be actuated for this condition.

Figure 1: Simple Pneumatic Temperature Control Loop



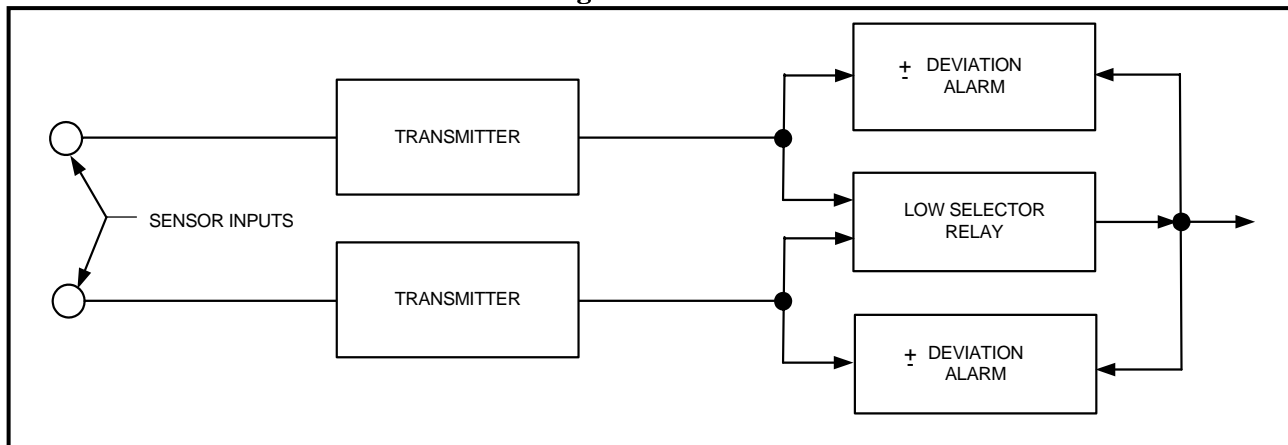
- E. In the above example (Item B), the addition of a low-signal detector (alarm) may appear to be a solution, but this does not provide protection for any condition except the abrupt loss of signal. A gradual loss of the signal will cause the controller to compensate by increasing the process temperature, but there will be no indication that an abnormal condition exists. The addition of a redundant alarm circuit connected directly to the sensor (primary element) would detect this condition and would be recommended for this circumstance.
- F. Where the use of a reverse action transmitter is preferred but not available, an alternative is the installation of a direct action transmitter close coupled with a reverse action relay. This may improve safety at the expense of system reliability and accuracy. This design, however, is inferior to a transmitter with built-in reverse action.
- G. Reverse action may be obtained from a standard differential-pressure transmitter equipped with an elevation suppression kit. In this application, the high and low inputs are reversed and the suppression is adjusted such that zero differential produces one hundred percent output and full span differential produces zero percent output, see Figure 2 below.

Figure 2: Differential - Pressure Transmitter Reverse Connected for Fail-Safe Operation



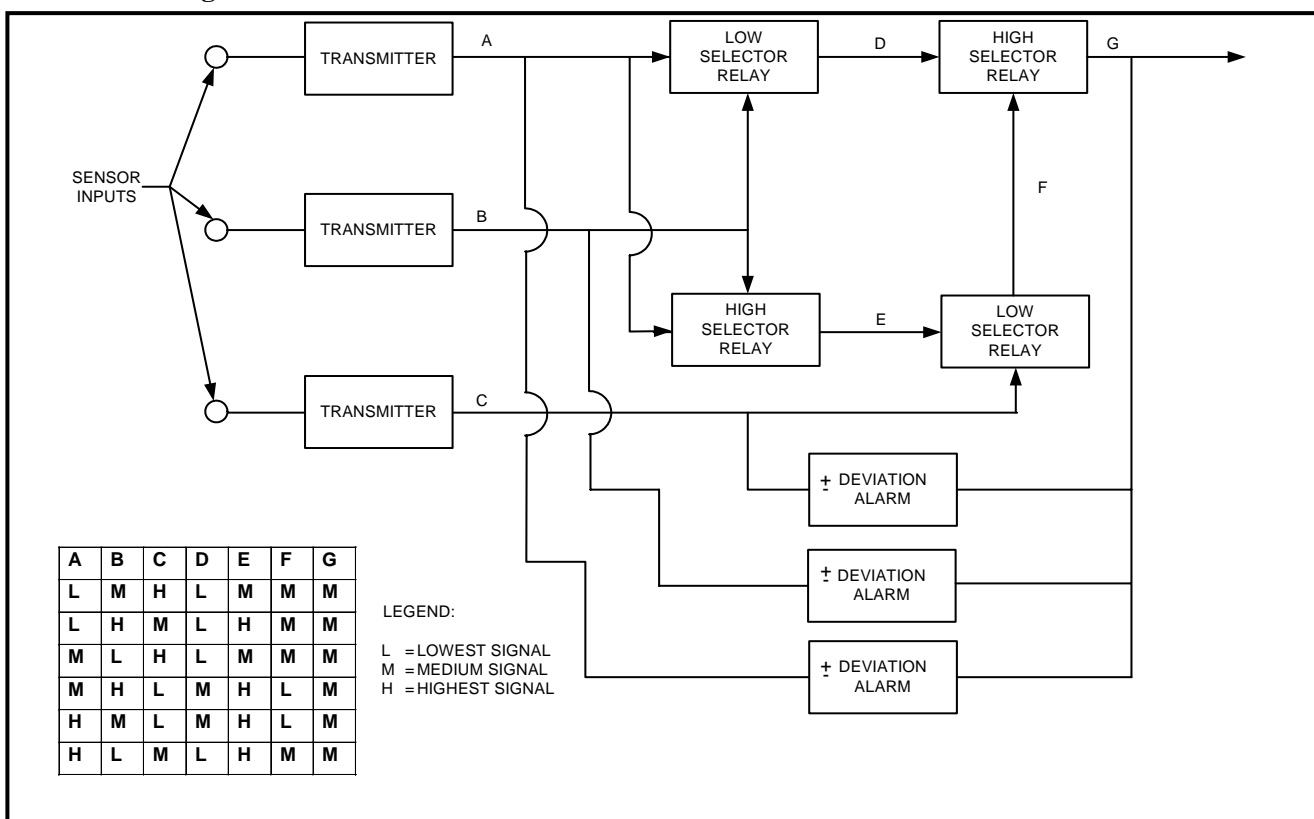
- H. The fail-safe analysis may reveal that transmitter failures or unpredictable sensor faults will defeat fail-safe objectives. In such instances redundancy should be considered in addition to the above mentioned fail-safe design guidance.
- I. The fail-safe design of a process control loop with redundant transmitters should consider the addition of a low select relay on the output of the transmitters. As shown in Figure 3 below, the low select relay detects the lowest output of the two redundant transmitters. The resulting value is then compared to the output of each transmitter. If the comparison yields a deviation that is not within a preset acceptable range, the deviation alarm will be activated indicating a lost in transmitter redundancy. The deviation alarms will also detect possible failures of the selector relay, which will generally cause a deviation large enough to activate the alarm. Only when both deviation alarms are tripped should an interlock shutdown be necessary.

Figure 3: Redundant Fail-Safe Transmitters With Low Selector Relay and Alarms for Higher Level of Protection



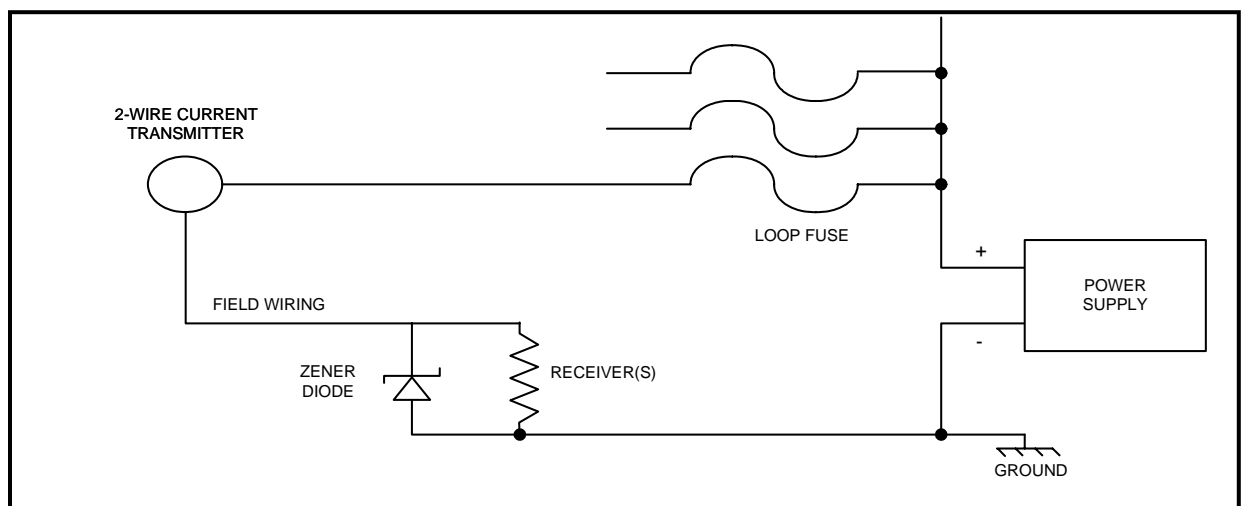
- J. A three-transmitter median selector system is shown in Figure 4 below. The median selector is made up of two high selector relays and two low selector relays. A plus or minus deviation alarm comparing each transmitter output with the final output detects a transmitter failure.

Figure 4: Three Parallel Transmitters with Median Selector and Alarms



- K. Components of a process control loop that are located within a hazardous area should be made intrinsically safe. A two-wire transmitter is shown in Figure 5 below with an intrinsically safe barrier. The addition of a zener diode and a fuse to the circuit protects against all but partial short circuits (leakage) across the transmitter terminals. The zener diode will not allow the voltage across the transmitter input to exceed the rated zener voltage. Excess voltage will cause the zener diode to conduct, which will blow the fuse. The zener voltage is selected so that conduction begins at a reasonable overrange of signal. Intrinsically safe transmitter circuits often add resistors in the loop to limit any fault current to a moderate overrange of signal. It may be difficult, however, to obtain a fuse that will blow under this circumstance.

Figure 5: Increased Protection for 2-Wire Systems



7.0 FAIL-SAFE CONTROLLER CONFIGURATION

- A. The fail-safe analysis should acknowledge that the failure mode of some digital controllers is unpredictable.
- B. Digital controllers implemented through a fail-safe design should have features such as self-diagnostics, field device diagnostics, internal redundancy, and integrated event recording and alarm notification.
- C. In the event of loss of power, most digital controllers can be configured for any of several different ways to restart on power restoration. Controllers also provide configurable options on whether or not to use set point tracking. While these combinations of features can provide some powerful advantages, some combinations of the selected configuration parameters could result in a possible unexpected and unsafe operation on restoration of power. The configuration of the controller should be carefully selected to obtain the desired fail-safe response of the process control loop.

8.0 FAIL-SAFE CONTROL ELEMENT CONFIGURATION

- A. It is essential that the final control element be properly specified to assure that failures in its signal or energy source produce a safe process state.
- B. The direction of action for a fail-safe control element (e.g., air-to-close or air-to-open) can be chosen based upon knowledge of the controlled variable. For example, if a valve positioner pressure booster relay, or current-to-pressure transducer is used, it should not reverse the relationship between the transmitted signal and valve actuator pressure. Loss of supply or transmitted signal should result in a safe direction of action for the control element.
- C. Loss of supply or transmitted signal should result in a safe direction of action for a control element. Process interlocks or alarm should be configured to alarm on loss of signal.

ENDNOTES:

ATTACHMENT 3

INSTRUMENTATION AND CONTROLS DESIGN REVIEW

(PROGRAMMATIC AND FACILITY)

TABLE OF CONTENTS

1.0	PURPOSE AND SCOPE	2
2.0	DEFINITIONS	2
3.0	GUIDANCE	3
	APPENDIX A: CONTROL SYSTEM DESIGN CHECKLIST	4

RECORD OF REVISIONS

Rev	Date	Description	POC	OIC
0	10/--/03	Initial issue	Mel Burnett, <i>FWO-DECS</i>	Gurinder Grewal, <i>FWO-DECS</i>

1.0 PURPOSE AND SCOPE

This attachment provides guidance for the conduct of design reviews of Instrumentation and Control (I&C) systems. The attachment provides the means to improve consistency, overall design, equipment specification, and lifecycle maintenance. It also provides guidance for addressing technology obsolescence.

2.0 DEFINITIONS

Component Location Identifiers – A labeling designation used to identify the location of a component. It generally consists of a combination of designations such as the component area, system, equipment type, and number.

Control Philosophy – A control system design approach that consists of: (1) establishing process control objectives (functional performance descriptions, process monitoring requirements, operational limits, etc.), (2) applying the most appropriate control techniques (ratio control, feed-forward control, cascade control, etc.), and (3) ensuring control system attributes (diversity, separation, isolation, redundancy, fault diagnostics, testability, etc.) are available for the reliable, efficient, and safe control of a facility / process.

Engineering Standards Task Matrix – An application matrix that provides for the selection of a minimum set of national codes and standards to be addressed for I&C systems. Refer to the I&C Chapter, Section 200 – D3060/F1050, Subsection 3.4.

Functional Classification – A graded classification system used to determine the minimum requirements for Systems, Structures, and Components (SSCs) (e.g. design, operation, procurement, and maintenance requirements). The four Functional Classifications in order of precedence are ML-1 and/or SC, ML-2 and/or SS, ML-3, and ML-4.

Instrument Range – The region between the limits within which a quantity is measured, received, or transmitted, expressed by stating the lower and upper range values. It is often expressed as the difference between the upper and lower measurable limits.

Instrument Scale – The graduated series of marking on an instrument display, usually used in conjunction with a pointer to indicate a measured value.

Instrument Sensitivity – The smallest change in actual value of a measured quantity that will produce and observable change in an instrument's output.

Measurement and Test Equipment (M&TE) – Portable or fixed equipment used for acceptance, calibration, measurement, gauging, testing, and/or inspection of equipment in order to control or acquire data to verify conformance to specified requirements or for reference information (monitoring and data collection).

Safety Significant Instrumented System – An SS system or 29 CFR 1910.119 hazardous process independent protection layer that requires instrumentation, logic devices and final control elements to monitor and detect an SS event, and which will result in automatic or operator action that will bring the facility or process system to a safe state.

3.0 GUIDANCE

- A. An appendix to this attachment (Appendix A) provides a checklist that can be used to address the quality of an I&C system design. The questions are worded such that the desirable answer is “Yes”. It is, however, understood that not all questions are applicable to all I&C systems. The number of questions that are applicable and are answered “Yes” will be indicative of the quality of design.
- B. Maximum benefit is obtained when the attached checklist is used throughout the design phase. Completing the checklist at the beginning of a design task insures that the proper considerations are given and can reveal inconsistencies in the design approach. The checklist should be used during design reviews to assess the extent of progress in meeting the intent of the questions. For the final design review, the checklist provides a means to assess the completeness and quality of the system design.

Appendix A: Control System Design Checklist

Obsolescence

1. Is there a provision in the bid specification for migration to newer technologies?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Does the supplier have a migration plan to newer technology covering the next 5 to 10 years?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Is there a good balance between proven and new technology? (e.g., Equipment is not approaching obsolescence, but is not untested technology either.)	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4. Are spare parts available as “off-the-shelf” items?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5. Has the supplier provided a product support plan that covers at least five years following product delivery?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6. Are there alternate sources available for the chosen components and are they compatible?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
7. Does the supplier have a good record of product support?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
8. Is the supplier considered to be a stable, viable supplier?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Consistency

1. Has the I&C system design been reviewed for consistency of design? (See five sub-questions below)	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
1.1 Can the system be operated and maintained without any significant additional site training for operations or maintenance personnel?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
1.2 Can existing facility procedures be utilized, or slightly modified in use, in order to operate the new control system?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
1.3 Can a common set of spare parts be used to maintain the proposed new system and exiting facility systems?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
1.4 In the event of multiple design groups or engineers, have difference segments of the new I&C system been designed so that the same control strategy is used	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
1.5 In the event of similar existing systems within the facility, has the new I&C system been designed so that it employs the same control strategy as the existing systems?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Does the I&C system design support a uniform and consistent operating philosophy? (See four sub-questions below)	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2.1 Are instruments that make similar measurements the same type of instruments? (e.g., all similar flows measured with the same type of flow meter?)	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

2.2 Are alerts/alarms/interlocks for similar functions applied, prioritized, and handled in a consistent manner?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2.3 Is process data being presented (display/engineering units/accuracy) in a consistent manner for similar applications?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2.4 Is the instrument scale consistent with instruments that make similar measurements?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Is the I&C system design consistent with the requirements established for the proposed functional classification?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4. Have Component Location Identifiers (CLI) been assigned in a consistent manner with other similar systems in the facility?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5. Are process displays consistent with applicable standards and existing conventions?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6. Is the new I&C system equipment compatible with existing telecommunications equipment?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
7. Is the new I&C system compatible with existing systems with which it interfaces?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
8. Are databases (e.g., instrument index, I/O, alarm setpoint) established in the design consistent with existing databases?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Technology

1. Has control software been developed in accordance with the specified facility software requirements?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Is the instrumentation the most appropriate for the type and range of measurement?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Can the supplier provide an upgrade path for the I&C components to provide compatibility with fieldbus architecture if applicable?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4. Does the I&C system utilize industry standard communication protocols instead of proprietary ones?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5. Does the I&C system have the capability to easily add more I/O points or drops?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6. Are on-line and/or self-diagnostics included in the system design?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
7. Does the system provide on-line help for operators and engineers?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
8. Can the system provide printouts of its configurations, logic, and executables for documentation purposes?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Good Design Practice

1. Is a control philosophy established for the facility?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Are commercial “off-the-shelf” products being used to the maximum extent in the new design?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Has energy efficiency been considered between design alternatives?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

4. Has the heat load on the HVAC system resulting from the installation of additional equipment been taken into consideration?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5. Has a human factors approach been applied in the design of operator workstations and any other Human Machine Interfaces?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6. Have power sources been identified for electrical load studies?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
7. Has the system been designed to be fail-safe?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
8. Has the National Codes and Standards Task Matrix been reviewed for applicable I&C design standards for the proposed functional classification?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
9. Has the system been reviewed for security requirements established for computer-based control systems?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
10. Have all instruments been placed so that they meet guidelines for accessibility and proper operation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
11. Have all instruments and actuators been sized to meet minimum, maximum, and nominal process operating conditions.	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
12. Has the instrument, instrument range, and instrument sensitivity been selected based on operational process sensitivity requirements?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
13. Has the design team agreed on the design standards that will be applied?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
14. Has space for expansion been provided if required for operation in the future?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
15. Are I&C materials of construction compatible with process materials and the operating environment?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
16. Has the system availability and reliability requirements been identified and met in the design?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
17. Has a life cycle cost analysis been performed and is the selected system competitive when compared to other designs?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
18. Has the supplier been qualified and placed on an approved supplier's list?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
19. Does the design specification include a factory acceptance test?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
20. Does the supplier specification require that the supplier be compliant with NQA-1 and that the supplier identify, in his proposal, all deliverables including lifecycle documentation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
21. Has the appropriate design requirements been applied to ML-2 / Safety Significant instrumented systems?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
22. Has the control system design been reviewed to ensure it does not interfere with existing monitoring, alarm, and safety systems?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
23. Is the proper level of receipt inspection included in the purchasing documents?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
24. Is documentation for the application of DOE G 420.0 standards provided?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

Maintenance

1. Has instrumentation been modularized where possible for low maintenance and repair costs?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
2. Does the purchase requisition require the vendor to supply specification sheets in hard and electronic copy?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
3. Does the design allow for maintenance to be conducted with minimum or no impact to plant operation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
4. Does the purchase requisition require the vendor to supply calibration certification, M&TE requirements, and procedures for any unique or special instruments?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
5. Has the Procurement Department's controlled product list been reviewed to ensure no suspect materials are being used as critical components?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
6. Are appropriate features available for calibrating / testing?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
7. Are items accessible and oriented for support by construction and maintenance?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
8. Can the system be maintained without special calibration equipment or procedures?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
9. Has weather protection been provided where necessary?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
10. Has the I&C system design taken into consideration ALARA issues for maintenance and operational personnel?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
11. Does the supplier offer training for maintenance personnel on its I&C components if necessary?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
12. Does the I&C system design incorporate features to limit system susceptibility to electrical noise, ground loops, static electricity, lightning strikes and electrical surges?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
13. Has the supplier demonstrated a good quality assurance program and a quality product? (e.g., Records do not indicate quality concerns with the supplier's products)	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A

ENDNOTES:

ATTACHMENT 4

INSTALLATION AND CALIBRATION OF INSTRUMENTS (PROGRAMMATIC AND FACILITY)

TABLE OF CONTENTS

1.0	PURPOSE	2
2.0	SCOPE	2
3.0	ACRONYMS AND DEFINITIONS	2
4.0	MATERIALS.....	4
5.0	PROCESS TAPS	4
6.0	INSTRUMENT LOCATION AND INSTALLATION GUIDANCE.....	4
7.0	INSTRUMENT SENSING LINE INSTALLATIONS	6
8.0	INSTRUMENT SENSING LINE PENETRATIONS	8
9.0	SUPPORTS / ANCHORS / GUIDES.....	8
10.0	INSTRUMENTATION VALVES	9
11.0	INSTRUMENT PANELS, RACKS, ENCLOSURES AND LOCAL MOUNTS	11
12.0	PRESSURE / FLOW CONSIDERATIONS	12
13.0	LEVEL CONSIDERATIONS.....	13
14.0	TEMPERATURE CONSIDERATIONS	14
15.0	SHIELD WALL PENETRATIONS	14
16.0	TESTS AND INSPECTIONS	14
17.0	CALIBRATION	15

RECORD OF REVISIONS

Rev	Date	Description	POC	OIC
0	10/--/03	Initial issue	Mel Burnett, <i>FWO-DECS</i>	Gurinder Grewal, <i>FWO-DECS</i>

1.0 PURPOSE

This attachment provides guidance for the mechanical installation and initial calibration of field installed instrumentation, equipment supports, and associated tubing systems.

2.0 SCOPE

This attachment applies to all I&C systems and devices and may be supplemented with specific installation and initial calibration requirements provided on design drawings or by other project specific documents.

2.1 Included

- Installation of instrument sensing lines and fittings
- Installation of instrument valves and manifolds
- Fabrication and installation of sensing lines and supports
- Location and installation of local, panel mounted, and rack mounted instruments
- Installation of instrument racks, panels, and enclosures
- Installation testing and inspection
- Location of instrumentation mounted in and on process equipment, vessels, or process piping
- Instrument calibration at component level

2.2 Not Included

- Installation and/or furnishing electrical raceway, conduit, cable and electrical terminations
- Periodic calibration
- Installation inspection and documentation of vendor installed instruments
- Installation of in-line mounted instruments
- Installation of control valves

3.0 ACRONYMS AND DEFINITIONS

3.1 ACRONYMS

ANSI - American National Standards Institute

ASME - American Society of Mechanical Engineers

HVAC - Heating, Ventilation and Air Conditioning

HP - High Pressure

ISA – The Instrumentation, Systems, and Automation Society

LP - Low Pressure

P&ID - Process and Instrumentation Diagram

RTD - Resistance Temperature Detector

3.2 DEFINITIONS

Calibration – The systematic process performed to determine outputs of a device corresponding to a series of values of the variable which the device is to measure, receive or transmit for the purpose of determining the error of the device compared against a standard and /or adjusting the device to bring it to the desired value, within a specified tolerance.

Cold Bend – Shaping tubing or piping by bending, drawing, stretching, or other stamping operations without the application of heat.

Design Agency – The organization performing the detailed design and analysis of a project or modification.

Design Authority – The person or group responsible for the final acceptability of and changes to the design of a system or component and its technical baseline (typically the manager of engineering).

Flaring – Increasing the diameter at the end of pipe or tube to form a conical section.

Gauge Glass – A glass or plastic tube for measuring liquid level in a tank or pressure vessel, usually by direct sight.

Impulse Line – The line, tubing or pipe, that connects the process to the primary measuring element of the instrument loop and is part of the process pressure boundary and containment. Sensing lines and impulse lines are the same.

In-Line Instrument/Device – Instrument/device installed in the process piping system (e.g., control valves, orifice plates, thermowell).

Installation Detail – Installation documentation in the form of standards, specifications, procedures, drawings, and quality inspection plans.

Instrumentation – A mechanical, electrical, pneumatic or hydraulic item (device/component/equipment) which is used for process monitoring or control. This also includes items such as sample probes and thermowells, which support instrumentation functions.

Line Mounted Instrument – Instrument installed in a connection attached to the process piping system (e.g., temperature indicators, temperature elements, temperature switches).

Local Mounted Instrument – Instrument installed locally on a wall, column, floor stand, etc. (e.g., transmitters, switches, indicators).

Pigtail – A 270° or 360° loop in pipe or tubing to form a trap for vapor condensate. Used to prevent high temperature vapors from reaching the instrument.

Root Valve – The first valve located in a sample line after it taps off the process. It is typically located in close proximity to the sample tap.

Seal Pot – Enlarged pipe sections in measurement impulse lines to provide a) a high area to volume displacement ratio to minimize error from hydrostatic head difference when using large volume displacement measuring elements, and b) to prevent loss of seal fluid by displacement into the process. A section of pipe (4 in. diameter) installed horizontally at the orifice flange union to provide a large area surge surface for movement of the impulse line fluid with instrument element position change to reduce measurement error from hydrostatic head difference in the impulse lines.

Snug Tight – Snug tight is a solid connection obtained using standard tools where bolting hardware has been sufficiently tightened to bring contacting surfaces of the bolted assembly into solid contact without damaging or distorting the assembly or hardware

Standpipe – A vertical tube filled with a liquid.

Thermowell – A pressure tight receptacle adapted to receive a temperature sensing element and provided with external threads or other means for pressure tight attachment to a vessel.

Wet-Leg – A liquid filled sensing line in a differential pressure level measuring system.

4.0 MATERIALS

- A. Before fabrication all materials should be visually examined for defects.
- B. Material should be controlled during construction at all times to ensure that it is identifiable as acceptable material.
- C. Tubing, fittings and valve ends should be sealed to prevent moisture, dirt and foreign matter from entering the tubing/valves during storage.
- D. Material should be compatible with the environment in which it is located. If contact is made with the process, the material should also be compatible with the measured medium at the specified operating conditions. Consideration should be given to the affects of corrosion, abrasion, contamination, and degradation due to excessive pressure or temperature.

5.0 PROCESS TAPS

- A. The general location of the process tap with respect to other taps/branches should be shown on a P&ID. The exact location of process connections may be shown on area piping composite drawings, piping isometric drawings, HVAC drawings, or the equipment vendor drawings.
- B. The placement of the tap on the process pipe should take into consideration instrument operability concerns, such as required number of pipe diameters up or downstream of a fitting / sensing device. If the tap can perform its function in a number of locations, choose the one nearest the sensing device.
- C. During the placement of the tap, strive for maintenance accessibility of root valves and a vertical stem installation.
- D. The process tap should be located near a pipe support to minimize vibration.

6.0 INSTRUMENT LOCATION AND INSTALLATION GUIDANCE

- A. The Design Agency should consider the following design aspects for location of instruments:
 - 1. Routing of sensing line from the process tap to the instrument
 - 2. Sensing line penetrations through walls and floors

3. Space requirements for installation, operation, maintenance, calibration, accessibility and electrical flex conduit installation
 4. Operational Environmental Specifications
 5. Vibration-free mounting on available structures
 6. Radiation level of mounting area. Instruments are to be located in low radiation and non-hazardous areas where possible
 7. Chemical Exposure
- B. Instruments should be installed such that servicing, calibration, or replacement can be made with a minimum of sensing line disassembly and with easy access to all connections.
- C. Local instruments, other than direct actuated indicators such as pressure gauges, should be mounted at an accessible location on columns, walls, or floor-mounted structures rather than mounted on process piping.
- D. Instrument mounting heights from the floor should be approximately 1.4 meters (4 feet-6 inches) for wall-mounted instruments and floor stand mounted instruments when measured from the centerline of the instrument. Deviations from the indicated location should be a maximum of ± 1.5 meters (± 5 feet) in plan, and ± 30.5 cm (± 1 foot) in elevation.
- E. Instruments should be located near operating spaces but should not obstruct aisles or walkways.
- F. Avoid locating instruments in areas where there is likelihood of damage to the instrument or instrument sensing lines. If instruments must be located in a potentially hazardous area, protective barriers should be installed.
- G. Gas and liquid pockets in liquid and gas sensing lines can be avoided with sufficient slope (See Item I, Section 7.0) and locating instruments relative to the process connection as follows:

Fluid	Preferred Instrument Location Elevation
Liquid	Below Line Connection
Steam over 138 Kilopascal Absolute (20 psia)	Below Line Connection
Steam not over 138 Kilopascal Absolute (20 psia)	Above Line Connection
Gas	Above Line Connection

- H. Instruments should be located such that the sensing lines are as short as practical to minimize slope requirement problems. Instruments that cannot be connected with proper slope should be provided with vent or drain points.

7.0 INSTRUMENT SENSING LINE INSTALLATIONS

- A. Instrument sensing lines should be installed in accordance with the guidance presented in this attachment, design drawings, and installation details. The safety classification of piping for instrument tubing systems should be, as a minimum, consistent with the requirements of the process system to which the instrument is connected.
- B. Sensing lines should not be installed in a manner that would interfere with or prevent maintenance and/or operational activities. Minimum headroom clearance of known and identified passageways should be 2.1 meters (7 feet).
- C. Whenever practical, sensing lines should be routed along walls, columns, or ceilings, avoiding open or exposed areas. Structural channels or a track should be installed to protect sensing lines in exposed locations subject to accidental crushing or damage. This type of protection, however, should not render the tubing and fittings inaccessible.
- D. Instrument sensing lines should be routed separately from process lines and equipment where vibration, abnormal heat, or stress could affect the lines. Tubing and piping that must be connected to vibrating equipment should be fabricated with adequate flexibility.
- E. Instrument sensing lines should not come in contact with structural steel and concrete surfaces of building members. In no case should tubing be installed in direct contact with painted or unpainted concrete surfaces, except for penetrations requiring closure. Grout should only be used for tubing with temperatures below 93° C (200°F).
- F. Instrument sensing lines routed through penetrations, shield walls or other barriers where visual contact is impaired or lost, should be labeled with a permanent tag attached securely on each side of that barrier displaying the corresponding instrument identifier.
- G. The spacing around sensing lines should always be wide enough to allow each tube to expand independently at all turns without striking adjacent tubes or other equipment.
- H. Heat tracing should be used for sensing lines containing liquid that may freeze or become viscous, or a wet gas from which moisture may condense. The heat tracing should provide enough heat to prevent freezing or condensation, but not great enough to boil the liquid in the sensing line.
- I. Sensing lines should have continuous slope to promote their being kept either full or free of fluid (unless noted otherwise). The preferred slope is 8.3 cm/m (1 inch per foot), however, 2.1 cm/m (1/4 inch per foot) is acceptable. For instruments sensing steam at pressures up to 138 kilo pascals absolute (20 psia), the instrument lines should slope a minimum of 16.7 cm/m (2 inches per foot). Minimum slope will begin after the root valve and terminate at the instrument valve inlet. The sensing lines may be level through and on each side of a valve manifold or instrument connection shut off valve for a distance of up to 10 cm (4 inches). Instrument sensing lines may be level through and on each horizontal leg of a vertically oriented tee or cross connection for a distance of up to 10 cm (4 inches), and through a penetration for a total cumulative length of 30 cm (12 inches) outside the ends of each penetration.

- J. Bends, rather than tube or pipe fittings, should be used to change the direction of sensing lines. The cold bending method is advised for all bends. A minimum bend radius of at least two and one quarter ($2 \frac{1}{4}$) times the tubing outside diameter should be employed for bends in stainless steel tubing and copper tubing. The minimum bend radius for capillary tubing, aluminum, and plastic tubing should be per manufacturer recommendations. Refer to the LANL Engineering Manual, Mechanical Chapter, for tube bending requirements and the determination of wall thinning effects.
- K. Where fittings must be used and an installation detail document specifies the size and type of fitting, a combination of fittings of other sizes may be substituted if the specified part is unavailable or it is more convenient to use the combination. The fittings must, however, be of the same equivalent type and produce the same or better overall effect. A weld fitting may replace a threaded or flareless joint, however, a threaded or flareless connection should not be used if welded fittings are required. Flareless fittings should be installed using the manufacturer's assembly instructions. For compression fittings, refer to LANL Construction Specification 15215, Compression Fittings on Copper and Stainless Steel Tubing.
- L. For threaded connections of stainless steel to stainless steel, lubrication should be applied to prevent seizing and galling. Low or no chloride content lubricants should be used with stainless steel. Although Teflon tape is allowed in many applications, it should not be used as a sealant or lubricant on threaded instrument connections. The use of compound or lubricant on threads should consider the potential reaction with either the service fluid or the piping material.
- M. Sensing lines should be blown clear of any foreign material with clean, oil free, dry air or nitrogen before the system is placed in operation. Demineralized water may be used to flush tubing, provided the process system to which the tubing is connected will also be flushed or hydro-tested with water in accordance with applicable construction procedures. Open lines, fittings or valves should be sealed after being blown clear. Instrument tubing between the manifold valve and the instrument is not required to be blown down or flushed if visual inspection is performed prior to final connection and tightening of fittings.
- N. Capillary tubes sealed to the instrument by the manufacturer should not be opened or cut during or after installation unless specifically required by the installation drawing or manufacturer's instruction. Slope requirements do not apply to capillary tubing. Manufacturer's installation requirements, including those relating to minimum bend radius, should be followed. Excess lengths of capillary tubing should be neatly coiled in protected enclosures. The maximum amount of unprotected capillary should be no more than 15 cm (6 inches) at any one location, except at capillary enclosures, process connections, instrument connections, and penetrations. At the entrance and exit of capillary enclosures, process connections and instrument connections, the maximum unprotected capillary should be 45 cm (18 inches). Capillaries in trays should be tied down or clamped every three feet. At the entrance and exit of penetrations, the maximum unprotected capillary should be 30 cm (12 inches).
- O. Primary sensing lines at local panels and racks should be neatly arranged with easy access to test, drain, and vent connections, instruments valves, and manifold. Primary tubing between the instrument valve or manifold and the instrument should be arranged in accordance with the vendor's instruction and with adequate flexibility to avoid undue strain to the instruments.

8.0 INSTRUMENT SENSING LINE PENETRATIONS

- A. Penetration closure materials should be considered for the effects on the free movement or restraint of instrument sensing lines. A support should be located within 91 cm (3 feet) of each end of the wall or floor. No supports are required through filled penetrations. All filled penetrations should be considered a 3 directional anchor.
- B. Where several instruments have sensing lines that share a common penetration, careful attention should be given to temperature effects. If adverse effects are possible, proper insulation or separate penetrations should be provided.
- C. Instrument sensing lines should not be routed with electrical conduit/tray through the same penetration.

9.0 SUPPORTS / ANCHORS / GUIDES

- A. Support intervals for sensing lines should not exceed those shown in the following table.

Outside Diameter	Material	Wall Thickness	Max Unsupported Span Metric
1/4"	Stainless & Carbon Steel & Copper	All	91 cm (3 ft.)
3/8"	Stainless & Carbon Steel & Copper	All	1.5 m (5 ft.)
1/2"	Stainless & Carbon Steel & Copper	All	1.5 m (5 ft)
3/4"	Stainless & Carbon Steel & Copper	All	1.8 m (6 ft.)
1"	Stainless & Carbon Steel	All	2.1 m (7 ft.)
Capillary Tubing	Carbon Steel & Copper	All	See Item N, Section 7.0

- B. Multi-tube bundles should be supported in accordance with the manufacturer's recommendations.
- C. Support structures for sensing lines should not be attached to instruments and should not be supported from or connected to root valves or root nipples.
- D. An instrument tray, angle iron, and/or channel should be used to minimize the number of supports required to support sensing lines. These options also provide protection for the sensing lines.
- E. Sensing lines should be supported by a combination of 3 directional anchors and 2 directional guides. A dummy tube should be installed in the unused hole of the 3 directional clamps. Clamps and fittings should not be installed within the arc of tubing bends.

- F. Anchors, consisting of connections to root valves, instrument valves, or any type of clamp that when fastened to tubing prevents axial movement of the tube, should be placed in each straight run of tubing that requires a support. The connection to the instrument is not considered an anchor point for this purpose.
- G. Sensing lines should be supported with guides wherever a longitudinal movement along the line axis is involved due to temperature, vibration, and related ambient conditions. When two or more tubes are attached to a single support, each line should be guided so that it can move axially independent of the others, unless the support is designed specifically as an anchor. It will always be assumed that each tube expands and contracts individually and independent of all others.
- H. For portions of a sensing line run which may be subjected to temperatures greater than 60°C, the following limitations apply:
 - 1. Anchors should be used only where the axial movement cannot be controlled easily by other means.
 - 2. Every effort should be made to support vertical runs and to control end movement of horizontal runs by thoughtful placement of guides near turns and offsets
- I. All fasteners should be at least snug tight. Bolted Fasteners, as a minimum, should have the end of a bolt to be at least flush with the outer surface of the nut. In the event that vendor instruction, design drawings or specification specify torque requirements, the vendor instruction shall take precedence. The torque values below should be used in the absence of specified values.

Bolt Diameter	Required Torque
Less than 1/4"	Snug Tight
1/4"	8.8 Nm (78 in lb) ± 0.7 Nm (6 in lbs)
5/16"	20 Nm (15 ft lb) ± 3 Nm (2 ft lb)
3/8"	29 Nm (22 ft lb) ± 4 Nm (5 ft lb)
1/2"	75 Nm (55 ft lb) ± 7 Nm (5 ft lb)
5/8"	81 Nm (60 ft lb) ± 8 Nm (6 ft lb)
3/4"	183 Nm (135 ft lb) ± 14 Nm (10 ft lb)
7/8"	183 Nm (135 ft lb) ± 14 Nm (10 ft lb)

* Nm = Newton Meter

10.0 INSTRUMENTATION VALVES

A. Vent, Drain and Calibration Valves

- 1. All normally closed valves should be installed with the flow arrow pointing in the direction of flow. For valves in static instrument lines the direction of flow should be considered away from the process tap so that when the valve is closed the pressure will be on the process side.

2. As a minimum, high point vents in liquid service sensing lines should be accessible by means of a portable ladder. Vent and drain valves in systems with normal operating temperatures greater than 49°C (120°F) should be labeled with an appropriate warning tag. Hazardous fluid systems, including cryogenics, should also be labeled with an appropriate warning.
3. All high points in liquid service sensing lines should have a valve vent connection located outside high radiation zones at an accessible elevation (if necessary at elevations accessible by means of a ladder). Vent valves should be located such that they are at the high point of the instrument line.
4. The use of hot blowdown for instrument lines should be avoided. Vents should be used for releasing trapped air, back flushing, or pre-filling of tubing systems. Vents should not be used for blowdowns. Lines subjected to temperatures above 93°C (200°F) should be designed for thermal expansion.
5. All vent and drain valves should be capped, plugged or have short pieces of tubing installed on the downstream side, unless specifically routed to a drain point. All drip legs should be a minimum of 61 cm (24 inches).
6. An accessible calibration connection should be provided between the instrument and its nearest isolation valve. The connection should be easily accessed for in-situ instrument calibration and servicing. This connection may be a vent or drain point provided that isolation from the process is acceptable. All such connections should be capped or plugged when not in use.

B. Root Valves

1. I&C design responsibility should begin at the outlet of the root valve.
2. When a root valve is located in a high radioactive or hazardous area, an accessible isolation valve should be provided.
3. The root valve should be installed clear of main line insulation in a horizontal or vertical orientation as required by specific conditions. Process connections and root valves should be located so that they are accessible.
4. For adapting stainless steel to main line class piping, socket welding should not be performed when the service temperature at a dissimilar weld is greater than 100°C (212°F). The methods of welding dissimilar materials in services above 100°C (212°F) should be provided by the Design Authority.

C. Isolation Valves

1. The instrument isolation valve is defined as the valve nearest the instrument.
2. A higher rated valve may be substituted for a lower rated valve of the same type (i.e., gate, globe, ball, etc).

3. An instrument line with a remote mounted instrument should have at least two valves between the process tap and the instrument. The root valve and instrument isolation valve will suffice, with the instrument isolation valve within reach of the instrument. For rack or panel-mounted instruments, the panel valve located at the panel process tap and the isolation valve located at the bulkhead will suffice. For locally mounted instruments, with the root valve within reach of the instrument, an additional isolation valve is not required.
 4. Isolation valves should be located just beyond a penetration on the non-radioactive side of a shield wall. This will allow instrument maintenance during plant operation when the root valve is inaccessible.
- D. All instrument valves (manifolds, vents, drains, isolations, etc.) in instrument process and sample tubing installations should be supported and considered a 3-directional anchor.

11.0 INSTRUMENT PANELS, RACKS, ENCLOSURES AND LOCAL MOUNTS

- A. Mounting instruments to the supporting structure should be in accordance with design engineering drawings, manufacturer's instruction, and/or details shown on vendor drawings. Deviation from the indicated location shall be ± 1.5 m (5 ft.) maximum plan and ± 30.5 cm (1 ft.) maximum elevation, unless otherwise noted on the drawings.
- B. Indoor field fabricated racks should be of open construction with welded steel plates, angles, channels, pipe, and unistrut or equal as illustrated within the appropriate installation detail.
- C. Outdoor field fabricated racks should be similar to the indoor racks but with a sheet metal enclosure if required by the instrument installation detail. Type NEMA 3S enclosure may be used for protection of instruments. The instruments should be weatherproof. Instruments requiring heat tracing and/or heated enclosures should be so indicated on P&ID and by the installation detail.
- D. Each rack which has more than one electrical instrument may be provided with a terminal box. Interconnection between the terminal box and instrument should be made with rigid steel conduit or seal-tight flexible conduit.
- E. Floor mounted racks (not supported by a wall at the top) should be mounted a minimum of 76 cm (2.5 feet) out from a wall, to provide working space during both construction and operation.
- F. When conditions require heated enclosures, instruments that must be heated should be in heated housings whose type and design allow for the following factors:
 1. Frequency of access
 2. Ease of access
 3. Availability of space
 4. Visibility of instrument
 5. Availability of heating medium
 6. Explosion hazard

7. Location of heat tracing connections
8. Insulation
9. Weather tightness
10. Weather resistance
11. The desired controlled temperature shall be a minimum of 45°F (7°C).

12.0 PRESSURE / FLOW CONSIDERATIONS

- A. In pressure measurement, the measuring device should come into direct physical contact with the process. However, special precautions should be taken if the process could potentially damage the device or be detrimental to instrument reliability. Consideration should be given to process temperature and pressure, corrosion, mechanical vibration, and process pressure pulsation. Pulsation dampers, insulation and bleed valves, seals and purges, as well as temperature insulation and heat tracing are options that may be necessary to maintain instrument reliability.
- B. For gas service, the sensing lines connecting the pressure instrument to the process should be free of liquid. For liquid and vapor service, the lines should be filled with liquid and void of any pockets of gas.
- C. The following is general guidance for differential-pressure instruments.
 1. Differential pressure sensing lines should be checked to make sure that they are connected to the proper sides of the instrument, High Pressure (HP) and Low Pressure (LP).
 1. Differential pressure sensing lines should be run together to the maximum extent practical so as to keep both lines at the same temperature. If they are insulated, they should be insulated together.
 2. The sensing lines for air or gas service should be self-draining so that condensate or impurities cannot accumulate on one side of the differential-pressure instrument.
 3. Differential pressure transmitters that are vented to atmosphere should have the vent connection constructed of solid material without a valve. The openings of vent connections should be in a downward direction to protect against falling particles. An insect screen should be installed at the end of the connection.
- D. The following is specific guidance for pressure and differential-pressure instruments in liquid, steam, or vapor service.
 1. The effects of hydrostatic head pressure caused by condensed liquid in the sensing lines should be considered when installing the pressure instrument. Since accessibility may not allow the instrument to be installed directly at the process, most instruments provide a zero adjustment to offset the effect of hydrostatic head pressures.

2. Condensate chambers, also known as seal pots, should be installed to ensure the instrument sensing lines are filled with liquid. Water or other coolants can be applied to the seal pots to speed the condensing process. The pipe from a process connection to a seal pot should be insulated for process fluids hotter than 121°C (250°F).
 3. The sensing lines to differential-pressure instruments should be installed to maintain the condensate legs at an equal height. A pair of seal pots should be at the same elevation ± 0.6 cm ($\pm 1/4$ inches) and as high or higher than the highest process connection.
 4. A pigtail or wet-leg should be considered to protect an instrument that may be subject to high process temperatures. The pigtail should be located close to the instrument. A wet-leg should have a filling connection, usually at the top.
 5. If there is a concern of moisture freezing in the sensing line, a diaphragm seal and low-temperature compatible fill fluid should be considered.
- E. Pressure calibration/test points should be accessible. If the root valve is not accessible (accessible defined as not over 1.8 m (6 feet) from floor, grating, or platforms), tubing and an instrument valve should be installed at a convenient remote location.

13.0 LEVEL CONSIDERATIONS

- A. For hydrostatic head level measurements, the High Pressure (HP) sensing line should be connected toward the bottom of the vessel but from the side. Connections from the bottom of the vessel are not recommended because of the possibility of trapping of solids in the sensing lines.
- B. Differential pressure level instruments should be located at the zero reference point on the vessel, unless a bubble system is used, in which case the instruments may be located at any convenient elevation. Refer to Item C in Section 12.0 for level differential-pressure instruments in steam or vapor service.
- C. A stilling well should be used where displacement or float-type elements are located inside a vessel subject to turbulence. A stilling well may be required to protect a bubble tube against excessive turbulence.
- D. Level devices should be placed away from areas of turbulence and should not interfere with other vessel parts or instruments, such as thermowells or sample nozzles.
- E. Stilling wells and bubble tubes should be firmly supported in accordance with the installation details. If they are to be removable, adequate room should be provided to allow them to be withdrawn.
- F. Gauge glasses should be installed adjacent to the vessel and whenever possible, should be visible from a walkway.
- G. Process connected level transmitters and indicators should be mounted within ± 2.5 cm (± 1 inch) of the design elevation. Liquid actuated level switches should be mounted within ± 0.6 cm ($\pm 1/4$ inch) of the design elevation.

14.0 TEMPERATURE CONSIDERATIONS

- A. Temperature elements for hazardous fluid applications should be installed in a thermowell unless otherwise shown by the design specification. Temperature elements installed without a thermowell should be identified with a “CAUTION - NO THERMOWELL” tag.
- B. The following design aspects should be considered for the location of thermowells:
 - 1. Temperature elements installed in process piping should be located where accessible for servicing, calibration, or replacement, and should not be located where vibration or shock is expected.
 - 2. Adequate space should be provided for the removal of thermocouples, RTDs, thermal bulbs or indicators from their protecting wells.
 - 3. Elements for steam service should be located so that they are not submerged in condensate.
 - 4. Elements for liquid service should be located so that they are submerged.
 - 5. Elements for air and gas service should be located so that they sense the true or average temperature and are not submerged in liquid.
 - 6. Installation of temperature elements into thermowells should be performed per vendor specifications to prevent element damage and ensure proper operation.

15.0 SHIELD WALL PENETRATIONS

- A. The following should be considered to avoid radiation streaming from instrument sensing line penetrations in shield walls:
 - 1. All instrument sensing line penetrations should be at a minimum height of 2.5 m (8 feet) above floor level.
 - 2. The tubing penetrations should be skewed toward an inner corner of the operating compartment where possible, avoiding a direct streaming path to the surrounding areas.
 - 3. If neither of the above is practical, the sensing lines penetrating the shield wall should be surrounded by a pipe sleeve with open space between the sensing line and sleeve filled with a suitable radiation absorbing material.

16.0 TESTS AND INSPECTIONS

- A. Pressure tests should include the instrument process tubing, instrument valves and fittings up to but excluding the instrument. The instrument connecting tubing should be capped or plugged prior to testing.
- B. Instrument tubing may be pressure tested along with the main process piping to which it is connected. Testing of individual instrument tubing systems may also be performed separately if found desirable.

- C. Tubing leaks in low-pressure systems may not be detectable through pressure tests. Additional leak tests should be considered for such systems.
- D. The instrument impulse tubing should always be tested to the same pressure as the process pipe system unless otherwise noted in the design specification. Test pressures can only be revised/waived by the Design Authority. Instrument air supply tubing should be tested at the same test pressure as the headers test pressure.
- E. The following attributes should be either inspected or functionally tested, and documented as appropriate for fabrication and installation. The responsible technical and quality personnel must determine the required detail and oversight that is necessary based on the safety classification of the I&C equipment / system.
 - 1. Verification of documentation from Construction Engineering
 - 2. Sensing Line Protection
 - 3. Sensing Line Slope
 - 4. Drain Connections
 - 5. Connection Lubricant
 - 6. Condensate Pot Elevation
 - 7. Stilling Well Location
 - 8. Mounted Panel & Racks
 - 9. Thermowell Installation
 - 10. Bends in Sample Lines
 - 11. Instrument Location
 - 12. Instrument Orientation
 - 13. Sample Tubing Supports
 - 14. Material Identification
 - 15. Instrument Tubing Supports
 - 16. Panels & Racks Location
 - 17. Blowdown / Flushing
 - 18. Pressure Testing

17.0 CALIBRATION

- A. Initial calibrations should be performed in accordance with the [Laboratory Calibration Program](#).
- B. As part of the initial calibration, the instrument details (i.e. manufacturer, model number, size, material of construction, range, etc.) should be verified to be in agreement with the design specification.

- C. The component under calibration should be subject to input variations at a number of test points ascending and descending to sufficiently verify its response over the full span. The following test points should be used when no other specific direction is given in the applicable procedure or work document.
1. Switches – Trip and reset. Switches for which no reset value is specified or which have fixed dead band, the reset value shall be documented on the calibration record for reference.
 2. Valves – Full open/Full closed; modulating valves should also be verified at mid-travel (50%)
 3. Mechanical and Electrical Indicator and/or Transmitter – at or near (within 10%) 0, 20, 40, 60, 80, and at or near 100% of span or reading increasing and 80, 60, 40, 20 and at or near 0% of span or reading decreasing.

ENDNOTES:

ATTACHMENT 5
ALARM MANAGEMENT
(PROGRAMMATIC AND FACILITY)

TABLE OF CONTENTS

1.0	PURPOSE	2
2.0	SCOPE	2
3.0	ACRONYMS AND DEFINITIONS	2
4.0	GUIDANCE	3
5.0	ALARM VALIDATION PROCESS.....	6
	APPENDIX A: ALARM VALIDATION PROCESS FLOWCHART.....	9
	APPENDIX B: ALARM SELECTION WORKSHEET.....	10

RECORD OF REVISIONS

Rev	Date	Description	POC	OIC
0	10/--/03	Initial issue	Mel Burnett, <i>FWO-DECS</i>	Gurinder Grewal, <i>FWO-DECS</i>

1.0 PURPOSE

This attachment provides guidance for assigning alarms to process monitoring and control systems and for implementing an alarm management strategy.

2.0 SCOPE

A method is provided to assign, prioritize, and document the basis of alarms used in the operation of a process facility. Fire alarms, security system alarms, and radiation alarms are not addressed. The design basis for controls and interlocks is not provided.

3.0 ACRONYMS AND DEFINITIONS

3.1 ACRONYMS

CLD – Control Logic Diagrams

CLI – Component Location Identifier

DCS – Distributed Control System

DHEC – Department of Health and Environmental Control

EN – Equipment Number

OSR – Operational Safety Requirement

PHR – Process Hazards Report

P&ID – Process & Instrumentation Diagram

PLC – Programmable Logic Controller

SAR – Safety Analysis Report

3.2 DEFINITIONS

Advisory – Information within the normal realm of operation that should be brought to the operator's attention, but does not require immediate operator action. Such information usually includes the maintenance status of plant equipment, automated systems, and interlocks.

If the operator is expected to determine an abnormal condition as part of his normal surveillance, then the condition should be presented to the operator as advisory information. As a Rule of Thumb, if transition of a process condition from normal to abnormal takes more than 30 minutes, an operator should detect it during normal surveillance. In general, advisories do not actuate a horn or buzzer.

Alarm – A process condition that requires operator notification so that action can be initiated by the operator to avert personal injury, equipment damage, safety and technical specification violations, environmental releases, or loss of function to process or safety systems.

Alarm Avalanche – An alarm avalanche condition occurs when a process event results in an overwhelming number of alarms. Such a condition usually makes it difficult or impossible for operating personnel to determine the nature of the event and to respond appropriately.

Alarm Prioritization Criteria – A set of established criteria used to classify an alarm based on the potential severity or impact of the alarm condition in a given process facility.

Alarm Review Team (ART) – Representatives from Engineering and Operations organizations assigned to review and approve alarm and interlock selection.

Alarm Selection Worksheet – A worksheet used to identify and document process alarms and their justification.

Alarm Validation Process – A systematic method for ensuring that alarm functions are properly selected and implemented.

Alert – Time dependent information indicating a trend in which lack of operator action could develop into an alarm condition. In general, alerts do not actuate a horn or buzzer.

Common Trouble Alarm – An alarm based on two or more abnormal conditions within the process. The alarm is usually triggered by the first of the abnormal conditions that occurs and returns to normal only after all abnormal conditions have cleared.

Guideline for Alarms – A set of practices to be followed in the identification and assignment of facility / process alarming functions.

Interlock – A process condition for which a process monitoring and control system takes automatic action to avert personal injury, equipment damage, safety and technical specification violations, environmental releases, or loss of function to process or safety systems.

If the operator does not have sufficient time to interpret an abnormal condition and take the required action, then an interlock should be configured in lieu of an alarm. As a Rule of Thumb, a process interlock should be considered for any transient from normal to abnormal conditions which takes less than 5 minutes, and should be required if it takes less than 2 minutes.

Multiple-Alarm-Event – A plant state that causes several alarm conditions to occur in a very short time period.

4.0 GUIDANCE

- A. Alarms are typically assigned in a process facility during design, although additional alarms are often added during commissioning, startup, and operations. Many alarms and interlocks are configured for specific facility, system, or component modes of operation. The resulting number of alarms presented to the operator may be excessive. Computer automation has exacerbated the situation by making it very easy to add new or change existing alarms. Too many alarms can lead to nuisance or redundant alarms, alarm avalanche conditions, or alarms that provide little or no assistance to operating personnel.
- B. An alarm validation process should be used to assign, configure, prioritize, and document the basis of alarms and interlocks in a process facility. This process should be implemented in stages to review and document the basis for both new and existing alarms / interlocks and define the scope of recommended improvements to the current alarm management system.

- C. An Alarm Review Team should be appointed to develop and implement the alarm validation process. The review team should consist of members representing both the operations and engineering organizations. The alarm validation methodology and the resulting recommendations should be approved by the review team, engineering, and operations management to insure that there is consistency between the current operating strategy, technical and safety requirements, and alarm response procedures.
- D. One member of the Alarm Review Team should be assigned as the Alarm Validation Coordinator. The Alarm Validation Coordinator coordinates the activities of the team; tracks candidate alarms and interlocks through the evaluation; maintains records of the review results and recommendations; and submits results to project management and operations for review and approval of design, set point, and procedure changes resulting from the validation process.
- E. The first step in the alarm validation process involves the identification of candidate and existing alarms / interlocks based on a review of the current technical baseline. The process then consists of documenting the justification, establishing set points, and establishing the method of detecting and responding (i.e. operator intervention vs. automatic interlock) to the event or condition. Instrument loops should be reviewed from a systems perspective to support existing alarms or recommend the addition or deletion of alarms. Process alarms and interlocks should be assigned as part of a facility monitoring and control strategy through an established Guideline for Alarms. The Guideline for Alarms should be developed to incorporate the accepted facility / industry standards and practices for implementing and handling alarms of generic process systems and alarm types. The following is an example of a typical set of guidelines that might be used for assigning alarms:
 - 1. Assign alarms only where the process operator must take a specific action directed to the process. Alarm response actions to “call someone” or some similar activity should not be used as a basis for an alarm. An alarm should not merely be informative (e.g., just to make sure the operator is aware of something).
 - 2. Assign alarms only for abnormal conditions over which the operator has control and / or responsibility.
 - 3. Delete unnecessary and redundant alarms if the process operator is already aware of the abnormal condition that led to the alarm. Specifically, if the answer to the following questions is “yes”, the alarm is considered redundant:
 - a. Is the operator already aware of the situation through normal surveillance activities?
 - b. Is the operator already aware of the situation through other alarms and interlocks?
 - c. Has the appropriate operator action been taken due to other alarms or interlocks?
 - 4. If an abnormal event of process origin (not including power failures, loss of instrument air, and the like) will generate two or more alarms, then consider the use of a common trouble alarm to address the multi-alarm event.

5. Assign alarms based on the following operator expectations:
 - a. If the transition of a process variable from near normal to abnormal is unlikely to happen within 30 minutes, then the process operator is expected to detect the situation as a part of normal surveillance activities.
 - b. If the alarm requires action by the operator in less than 5 minutes after the alarm condition is generated, then a process interlock or other automatic mechanism of response should be implemented in lieu of an alarm.
 6. Suppress alarms that are not meaningful during specific operation or maintenance modes.
- F. For facilities with many alarms, Alarm Prioritization Criteria should be established that reflects the relative severity of the condition or event indicated by an alarm. Priority levels should be established to reflect the importance of various alarm conditions in a given process facility. Each alarm should be assigned a priority based on the criteria. The alarm priorities can then be incorporated into the facility's alarm management system and procedures to assist operating personnel in identifying and responding to the most critical alarms. The following is an example of a typical set of Alarm Prioritization Criteria that might be used.

Priority 1 Alarm – Priority 1 alarms should warn operators of the most significant events requiring operator action. These alarms are generally safety based, however, depending on the nature of the process facility they may be based on critical regulatory, product quality, or economic criteria. For example, in a nuclear process facility, a Priority 1 Alarm might be used to warn the operator that there is a potential for a significant release of radioactivity or hazardous chemical that might affect the health and safety of employees and the general public. Alarms of this priority usually necessitate the manual shutdown of the process.

Priority 2 Alarm – Priority 2 alarms should warn the operator of less significant events than Priority 1 Alarms. As an example, these events could indicate the potential for transition to an unsafe condition, exceeding a regulatory or quality limit, or interrupting process operation. Priority 2 Alarms usually require action by the operator to mitigate the condition while maintaining process operation.

Priority 3 Alarm – Priority 3 alarms should warn the operator of less significant events than Priority 2 alarms. As an example, these events might include the potential to damage equipment, interrupt process operation, and/or exceed product quality limits. Alarms of this priority are based primarily on economic impact and require operator intervention to avoid a shutdown, equipment repair, etc.

Alert – An Alert provides an indication to the operator that the process is approaching an alarm condition, which may be avoided by appropriate operator action. Typically return-to-normal corrections are made through routine operations and procedures.

Advisory – An Advisory indicates a failure or status change that does not impact the ability to continue normal operation in a safe manner. No operator action is required.

- G. Once alarms have been identified and prioritized, an Alarm Validation Process should be applied to determine whether an alarm, interlock, or advisory is appropriate based on the time and information available for an operator to respond to an abnormal condition. This criteria addresses facility specific issues such as the need for hardwired alarms / interlocks, the use of automatic versus manual action, and handling multiple alarm conditions.

5.0 ALARM VALIDATION PROCESS

- A. The implementation of a detailed alarm validation process can be established through the performance of the following steps. A Flowchart is provided as an appendix to this attachment (Appendix A) to provide a graphic representation of the validation process.

- Step 1: Review pertinent technical documentation for alarm and interlock requirements. These may include P&IDs, CLDs, Loop Sheets, System Design Descriptions, Software Requirement Specifications, Set Point Documents, SARs, PHRs, OSRs, Process Requirements, DHEC and DOE requirements.
- Step 2: Apply the Guideline for Alarms to determine what alarms / interlocks are required for the process system, see Item E in Section 4.0 above.
- Step 3: Identify candidate alarms, interlocks, and set-point values noting the process system, instrument number (EN or CLI), instrument loop description, and type of installation (e.g., DCS, PLC, or Hardwired).
- Step 4: Apply the Alarm Prioritization Criteria developed for the facility, see Item F in Section 4.0 above.
- Step 5: Determine if Priority #1 alarm criteria is satisfied. If so and the alarm /interlock is part of or impacts the operation of a safety function, then it is recommended that implementation results in a highly reliable design.
- Step 6: Determine if Priority #2 alarm criteria is satisfied.
- Step 7: Determine if Priority #3 alarm criteria is satisfied.
- Step 8: Determine if only an Alert is needed. If so, proceed to the last step.
- Step 9: Determine if only an Advisory is needed. If so, proceed to the last step.
- Step 10: If the answers to Steps 5 through 9 are all “No” and notification currently exists, then it is recommended that the notification be removed from the facility.
- Step 11: If the answer to Steps 5, 6, or 7 is “Yes”, then it should be determined whether the alarm is required for only certain modes of operation. If so, the alarm should be linked with operational mode criteria to mask the alarm when it is not valid. An example would be when a low flow alarm is provided for a pump, the alarm would be masked or blocked when the pump was not running.

Step 12: If an interlock is provided to respond to an abnormal condition due to operational preferences or human limitations, the following items should be considered in the justification of a Priority #1, #2, or #3 alarm.

1. Refer to the P&IDs, CLDs, and Guideline for Alarms to assist in evaluating the requirement for the interlock. If it is determined that an interlock is required but has not been implemented for an existing process / facility, then compensatory measures should be placed into effect until the interlock is incorporated. If no interlock is required then an alarm is valid.
2. If an interlock exists and the operator can take action to correct the abnormal condition before the interlock occurs, then the alarm is valid. The interlock may not be necessary and should be considered for removal. As a Rule Of Thumb, an operator usually needs at least 5 minutes to recognize an abnormal condition and take action. If operator action cannot prevent the interlock, then justification for the alarm needs further consideration.
3. If the operator is required to take additional actions after an interlock occurs to lessen the severity of an event or to provide immediate notification of the event, then an alarm is valid. If no operator action is required, then an Alert or Advisory indication should be considered.

Step 13: If an abnormal condition generates two or more alarms, the alarms may be considered redundant. Examples of redundant alarms are:

1. Two or more alarms from redundant field instruments that monitor the same process variable.
2. Two or more alarms from independent field instruments that monitor process related variables.
3. Two or more alarms from field instruments that monitor independent process variables that exceed their alarm limits in rapid succession, as a result of one particular abnormal event condition.

Note: The criteria for alarm redundancy should not be applied to loss of power, instrument air, or other loss of service conditions that in general are multi-alarm events.

If the alarm is determined to be redundant, a determination should be made to see if a single common alarm could replace two or more redundant alarms. Examples of grouped (“ganged”) alarms are:

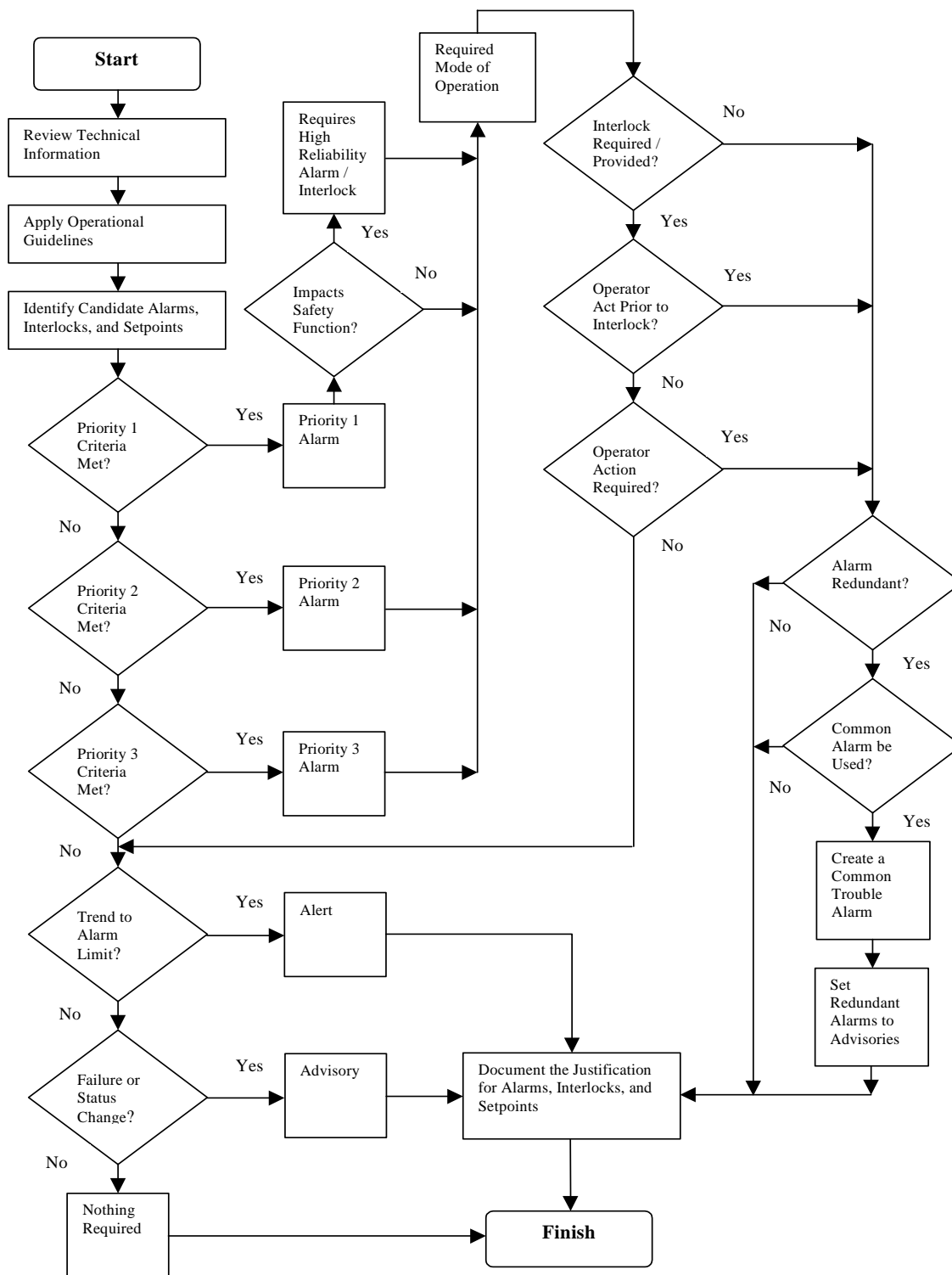
1. A common Low Tank Temperature Alarm and a common High Tank Temperature Alarm.
2. A common Loss of Flame Alarm.
3. A common Filter Plugging Alarm.

Step 14: Create a common alarm based on the redundant alarms. If redundant alarms are needed as advisory information for the operator, classify them as Advisories.

Step 15: Document the alarm functionality and required operator alarm response.

- B. Alarm Selection Worksheets are recommended to maintain a record of the alarm validation process and to document the design basis for new alarm s and changes to the current alarm configuration resulting from the application of the validation process. A typical example of an Alarm Selection Worksheet along with Instructions is provided as an appendix to this attachment (Appendix B).

Appendix A: Alarm Validation Process Flowchart



Appendix B: Alarm Selection Worksheet

Alarm Validation Process Procedure # _____ Rev. _____ Date: _____

1	Equipment No.: CLI No.: Type of Instrument Loop: DCS PLC Hardwire Other: _____
2	Process System Loop Description: (Descriptive Title of Instrument Loop and Variable)
3	Alarm Setpoint: (Value and Engineering Units) Set Point Type: (Example: High-High, Low-Low)
4	Interlock Required: (Identify Interlock Requirements)
5	Alarm Priority Level: (Determined by the Validation Process) Priority 1 Priority 2 Priority 3 Alert Advisory None
6	Applicable Modes of Facility Operation and Maintenance: (Example: Startup, Steady State Operation, Two Trains Running)
7	Recommended Changes Resulting from Validation Process:
8	Description of Alarm Functionality and Required Operator Alarm Response:

Facility Operations Manager Approval _____ Date: _____

Design Authority Approval _____ Date: _____

Alarm Review Team Approval _____ Date: _____

Appendix B: Alarm Selection Worksheet**INSTRUCTIONS:**

The Design Authority Engineer should enter the number and revision level of the Alarm Validation Procedure, the date the review was completed, and fill in the information in Sections 1 through 8 of the Alarm Selection Worksheet as described below for each alarm / interlock:

- Section 1: Enter the CLI and EN number for the component generating the alarm / interlock. Indicate how the alarm / interlock is implemented (e.g., DCS, PLC, or Hardwire).
- Section 2: Enter a description of the process and the measured variable (e.g., HEPA Filter Pressure Drop).
- Section 3: Enter the set point value and type (e.g., Setpoint = 30°C, High / Low Alarm).
- Section 4: If an interlock is involved, describe the interlock action.
- Section 5: List the priority as determined by the Alarm Validation Process.
- Section 6: List the operating and maintenance modes that the alarm or interlock should be active.
- Section 7: Document proposed changes resulting from the Alarm Validation Process (i. e. delete, make an advisory, hardwire, change priority, make common alarm).
- Section 8: Document the alarm functionality and required operator alarm response.

After completing the information, the Design Authority Engineer will sign the Alarm Selection Worksheet and submit it to his manager for review.

The Design Authority Engineering Manager will submit completed Alarm Selection Worksheets to the Alarm Review Team for review and approval.

If the Alarm Validation Process affects an existing facility, then the Design Authority Engineering Manager will submit the Alarm Selection Worksheets to the Facility Operations manager for review and approval.

ENDNOTES:

ATTACHMENT 6
INSTRUMENT LOOP DIAGRAMS
(PROGRAMMATIC AND FACILITY)

TABLE OF CONTENTS

1.0	PURPOSE AND SCOPE	2
2.0	DEFINITIONS	2
3.0	DIAGRAM FORMAT AND LAYOUT	2
4.0	DIAGRAM CONTENT	2
5.0	DIAGRAM SYMBOLS	3

RECORD OF REVISIONS

Rev	Date	Description	POC	OIC
0	10/--/03	Initial issue	Mel Burnett, <i>FWO-DECS</i>	Gurinder Grewal, <i>FWO-DECS</i>

1.0 PURPOSE AND SCOPE

This attachment provides guidance in the preparation and use of instrument loop diagrams. For additional guidance and examples refer to ISA-5.4-1991, Instrument Loop Diagrams.

2.0 DEFINITIONS

Instrument Loop Diagram – An engineering drawing which symbolically represents a single control loop identifying control components and interconnections. Special situations may necessitate a combination of loops on one drawing. A loop diagram may document electrical or pneumatic instruments or a combination of both.

P&ID – Process and Instrumentation Diagram

3.0 DIAGRAM FORMAT AND LAYOUT

- A. Size of Drawing: Loop diagrams should be prepared as 11-inch × 17-inch drawings. The smallest letter size should not be less than 1/8-inch.
- B. The loop diagram will generally contain only one loop. Special situations may necessitate a combination of loops on one drawing. The drawing should be arranged to prevent congestion and should provide extra space for future revisions. Complex loops that require more than one sheet may be expanded to as many 11" × 17" sheets as necessary. Adequate continuation points should be provided for proper understanding of the total loop configuration.

4.0 DIAGRAM CONTENT

- A. All components should be clearly labeled and uniquely identified.
- B. All components of the loop and the loop itself, including connections to multi-point and trend recorders and computers, should be identified (all instrument numbers should agree with the P&ID).
- C. The loop diagram should include word descriptions of loop functions. The title should be adequate, but if not, supplemental notes should be added. Descriptions of special functions and features that are not obvious, especially safety and shutdown circuits, should be given. All interconnections with electrical cables, conductor pairs, pneumatic multi tubes, and individual pneumatic and hydraulic tubing should be shown (this includes junction boxes, terminals, bulkheads, ports, and computer input/output, such as I/O connections, grounding systems, grounding connections, and signal levels). All interconnections should be uniquely identified and clearly labeled.
- D. The location of devices should be identified using descriptors such as field, panel front, panel rear, auxiliary equipment, rack, and termination cabinet.
- E. Electrical power, air and hydraulic supplies, including the designated voltage and pressure values, should be shown.

- F. The process lines and equipment should be sufficient to describe the process side of the loop and clarify the control action. Provide the process variable being measured and what is being controlled.
- G. Supplemental drawings and records should be referenced to show interrelations with other control loops, such as overrides, interlocks, cascades, and shutdowns.
- H. Although loop design often requires input from several different design areas, design responsibility and configuration control of the loop should be centered within a single function, such as the I&C group or Design Authority.
- I. Descriptions should be given for controller action, control valve action, control valve fail-safe action (electronic and/or pneumatic failure), and solenoid valve action.
- J. Calibration information should be shown in consistent units.
- K. Unique identification numbers consistent with other record documents should be shown for equipment such as racks, panels, and junction boxes.

5.0 DIAGRAM SYMBOLS

- A. Symbols used in instrument loop diagrams are provided in ANSI/ISA-5.1-1984, Instrumentation Symbols and Identification, and ISA-5.3-1983, Graphic Symbols for Distributed Control / Shared Display Instrumentation, Logic and Computer Systems.

ENDNOTES:

ATTACHMENT 7
CONTROL LOGIC DIAGRAMS
(PROGRAMMATIC AND FACILITY)

TABLE OF CONTENTS

1.0	PURPOSE AND SCOPE	2
2.0	DEFINITIONS	2
3.0	DIAGRAM FORMAT AND LAYOUT	2
4.0	DIAGRAM USES	2
5.0	DIAGRAM CONTENTS	3

RECORD OF REVISIONS

Rev	Date	Description	POC	OIC
0	10/--/03	Initial issue	Mel Burnett, <i>FWO-DECS</i>	Gurinder Grewal, <i>FWO-DECS</i>

1.0 PURPOSE AND SCOPE

This attachment provides guidance in the preparation and use of control logic diagrams. For additional guidance and examples refer to ISA-5.2-1976 (R1992), Binary Logic Diagrams for Process Operations.

2.0 DEFINITIONS

Control Logic Diagram – A diagram that provides easy to read graphic representation of the operation of individual system equipment controls using basic digital logic symbols. These symbols functionally relate manual and process input action to the process control and operator display output actions. The diagram does not imply the hardware to be used or describe the instrument signal levels involved. It serves as a basis for other drawings, such as electrical elementaries and schematics as well as for solid-state logic systems.

3.0 DIAGRAM FORMAT AND LAYOUT

- A. Size of Drawing: Control Logic diagrams should be prepared as Type 2 (11-inch × 17-inch) or Type 3 (17-inch × 22-inch) drawings. The smallest letter size should not be less than 1/8-inch.
- B. The control logic diagram should be arranged such that it is not congested or cluttered, is easily readable, and has extra space for future revisions.
- C. The overall logic flow of the drawings should be from left to right.
- D. Solid right angle lines should be used to connect the logic symbols. Line connections should be indicated by dots.
- E. Arrowheads should be used where the flow of logic is not in the normal direction, and where added clarity is needed.

4.0 DIAGRAM USES

- A. The functional operation of system equipment controls should be presented within Control Logic Diagrams so that it can be easily understood. The value of Control Logic Diagrams is lost if the basic functional operation is obscured by excessive detail.
- B. A control logic diagram provides an illustration of the logical design of the control system. Notes and references are also included to clarify the specific and overall system function.
- C. Control Logic Diagrams are to be used in conjunction with, not in place of, Process and Instrument Diagrams, Loop Diagrams, Schematic (Elementary) Diagrams, Interconnection Diagrams, Instrument Index, Data Sheets, and Vendor Drawings.

5.0 DIAGRAM CONTENTS

- A. The diagram contains graphic symbols that are interconnected to describe the logical relationships among different process equipment or calculated inputs and outputs. Symbols used in control logic diagrams are provided in ANSI/ISA-5.2-1976, Binary Logic Diagrams for Process Operations.
- B. The diagram should show only one or two items of equipment per drawing. For complex interlocks between individual items of a system, a single sequence diagram should be shown with a separate sequence block for each step. Each sequence block should reference a specific detailed control logic diagram that describes that block's function.
- C. Notes should be used to omit repetitive details and to clarify complex functions or operations. Two types of notes are typically provided on the specific logic diagram, general and specific. These type of notes are described as follows:
 - 1. General notes are brief statements that explain the control system function and provide hardware detail. They include general information and assumptions that apply to each control logic diagram. The notes do not need to be included on the drawing itself, but a reference to the document in which they reside should be given. Examples of some typical general notes are:
 - a. Logic symbols represent system functions only and do not normally show circuit arrangement, devices, or physical installation. They also do not define logic levels or other circuit operation states.
 - b. Process equipment will remain in, or return to, the original state after a loss and restoration of power, unless otherwise noted.
 - c. Inherent equipment interlocks, such as trip-free circuit breakers, are not shown.
 - d. The memory, reset, and start permissive logic associated with the operation of electrical protection devices is not shown. Electrical auxiliary system breakers are reset by operation of the control room or remote switch to trip. Mechanical auxiliary system circuits are reset by operation of a switch at the switchgear or motor control center.
 - e. The logic to show valve and damper position lights when the equipment is in an intermediate position is not shown.
 - f. Limit and torque switches to stop valve and damper motor actuators at the end of travel are not shown in the logic. The valve type and required action will be noted on the diagram when available.
 - g. Logic flow is generally from left to right. Symbols are oriented with inputs on the left and outputs on the right.

2. Specific drawing notes are included, when necessary, to clarify a particular function or to provide a more detailed description of the equipment used in the system. These notes should be referenced by number and included on the drawing. Some typical applications for specific drawing notes are:
 - a. Provide a brief statement of system startup, operation, and shut down functions.
 - b. Describe the purpose of a specific interlock.
 - c. Describe process and control equipment failure modes.
 - d. Describe process equipment response to loss and restoration of power (this could also be shown as an input to the logic).
- D. The following general rules should be followed when preparing a control logic diagram.
 1. Identify instruments, control switches, and equipment. The identification numbers should be identical to those shown on the Process and Instrument Diagram(s).
 2. Process inputs should indicate the condition at which they will function, such as low pressure or high level. The set points should not be included, unless specifically required to understand the logic diagram. A reference to setpoint documentation may be included as a reference.
 3. Each input circuit or contact should be shown as a separate logic input.
 4. Manual switch operation, nameplate arrangement, and location should be shown.
 5. Logic for each operating state of the equipment should be shown.
 6. Output actions should be clearly defined, such as “stop main pump”, “energize solenoid valve”, etc.
 7. All operator displays, such as indicating lights, annunciator inputs, and computer inputs, should be shown along with the location.
 8. Complex timing functions should be combined into one timing block instead of a combination of blocks. The time setting or expected range for timing blocks should be provided on the drawings.
 9. Any switching (backup power, redundant device, etc.) that occurs during faults and failures should be shown if applicable.
 10. A mid-point status can be placed in the diagram if useful as a reference in a sequence.
 11. If several systems contain the same equipment that operates in the same manner, one control logic drawing should be created with the device number differences noted in a table.
 12. Repetitive functions are typically identified on control logic diagrams with notes used to describe the function.
 13. Trip memory, reset, and start permissives that are used for mechanical device protection through physical inspection before restarting should be shown since they are non-repetitive.

14. Electrical protection circuits, memory, and start permissive interlocks are typically not shown. The specific circuits can be shown on schematic diagrams or as a detail on the control logic diagram.
 15. Similar equipment and functions should be controlled and presented in a consistent manner.
 16. A reference should be given for any related Process and Instrument Diagram, Schematic Drawing, or Vendor Logic Diagram.
 17. The control logic diagrams can be more or less detailed depending on its intended use. For example: The logic that shows the state a device will enter when simultaneous conflicting signals occur, such as start and stop, can be described graphically or through specific notes.
- E. In order to promote uniform diagramming of similar logic functions, the following terminology should be used where applicable.
1. “Start” and “Stop” should be used for manual logic inputs that are applied to mechanical equipment such as pumps or fans.
 2. “On” or “Off” should be used for equipment such as heaters.
 3. “Close” and “Trip” should be used for electrical system circuit breakers.
 4. “Electrical Protection” should be used to describe inputs that involve any short-circuit current, over-current, torque protection, or motor high temperature protection provided for electrical equipment.
 5. “Mechanical Protection” should be used to describe all process logic inputs that protect mechanical equipment, such as loss of suction pressure or high vibration.
 6. Control logic diagrams should be labeled and noted properly to avoid possible misinterpretation. For example, when describing a device such as a valve that may have two distinct states, indicate that it is “open” or “closed”. Stating that the valve is “not closed” or “not open” could be interpreted to mean that the valve is in an intermediate state.

ENDNOTES: